Hosted Email Security

Guida dell'amministratore

Protezione integrata della posta elettronica dalle minacce in un servizio in hosting

Trend Micro Incorporated si riserva il diritto di apportare modifiche a questa documentazione e a Hosted Email Security, in essa descritto, senza alcun obbligo di notifica. Prima di installare e utilizzare Hosted Email Security, esaminare i file readme, le note sulla release e/o l'ultima versione della documentazione applicabile, disponibili sul sito Web di Trend Micro all'indirizzo:

http://docs.trendmicro.com/it-it/smb/hosted-email-security.aspx

Codice documento: HSIM15998/130719

Data di pubblicazione: Settembre 2013

Protetto da brevetto USA N. 5.623.600, 5.951.698, 5.983.348, 6.272.641

Questa documentazione presenta le caratteristiche principali di Hosted Email Security e/o fornisce le istruzioni di installazione per un ambiente di produzione. Leggere questa documentazione prima di installare o utilizzare Hosted Email Security.

Altre informazioni dettagliate sull'utilizzo di funzioni specifiche di Hosted Email Security potrebbero essere disponibili nella Guida in linea di Trend Micro e/o nella Knowledge Base nel sito Web di Trend Micro.

Trend Micro si impegna continuamente a migliorare la propria documentazione. Per domande, commenti o suggerimenti riguardanti questo o qualsiasi documento Trend Micro, scrivere all'indirizzo docs@trendmicro.com.

È possibile esprimere un giudizio sulla documentazione al seguente indirizzo:

http://www.trendmicro.com/download/documentation/rating.asp

Contenuto

Prefazione

Capitolo 1: Introduzione a Trend Micro Hosted Email Security

Capitolo 2: Utilizzo Hosted Email Security

Capitolo 3: Gestione dei criteri

Capitolo 4: Mittenti approvati, quarantena e registri

Capitolo 5: Amministrazione e reputazione IP

Appendice A: Domande frequenti

Appendice B: Informazioni di contatto e risorse basate sul Web

Appendice C: Introduzione a Web EUQ

Glossario

Indice

Prefazione

Prefazione

Benvenuti nella *Guida dell'amministratore Hosted Email Security di Trend Micro*™. Che contiene informazioni sulle impostazioni e sui livelli dei servizi.

Gli argomenti trattati nella presente prefazione includono:

- *Novità* a pagina viii
- *Hosted Email Security Documentazione* a pagina viii
- *A chi si rivolge* a pagina ix
- *Convenzioni del documento* a pagina ix

Novità

Le funzioni aggiunte recentemente a Trend Micro Hosted Email Security includono:

- Indirizzamento della posta e interruzione del dominio (luglio 2013), vedere pagina 5-17.
- Integrazione con Trend Micro Licensing Management Platform (febbraio 2013), vedere la Guida in linea per ulteriori informazioni (http://docs.trendmicro.com/all/smb/hes/vAll/it-it/help/licensing_management_platform.htm).
- Possibilità di aggiungere più di un host come destinazione o server posta in uscita (novembre 2012), vedere pagina 5-17.
- Registri di verifica posta (eventi) dettaglio (giugno 2012): vedere pagina 4-16.

Hosted Email Security Documentazione

La documentazione di Hosted Email Security è formata dai seguenti elementi:

Guida in linea: consente di configurare tutte le funzioni attraverso l'interfaccia utente. Per accedere alla guida in linea aprire la console Web e fare clic sull'icona della guida ( ).

Guida dell'amministratore: consente di impostare e configurare tutte le impostazioni del servizio.

Nota: A partire dalla versione del 15.03.10, il nome di servizio "InterScan Messaging Hosted Security" viene modificato in "Hosted Email Security".

Guida ai servizi Web: permette di automatizzare le attività di amministrazione Hosted Email Security.

Guida utenti finali di Web End User Quarantine: fornisce informazioni sulla modalità di gestione dei messaggi di spam in quarantena mediante l'utilizzo del servizio Web End User Quarantine di Trend Micro.

La *Guida dell'amministratore* e la *Guida di Web End User Quarantine* sono disponibili all'indirizzo:

http://it.trendmicro.com/it/products/enterprise/hosted-email-security/support/index.html

A chi si rivolge

La documentazione è stata scritta per i responsabili IT e gli amministratori e-mail. Si presume che il lettore conosca in modo approfondito le reti di messaggistica e-mail, compresi i dettagli relativi a:

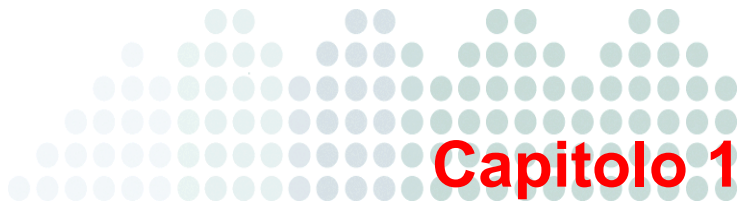
- Protocollo SMTP
- Agenti di trasferimento messaggi (Message Transfer Agents, MTA)

Non viene invece dato per scontato che il lettore abbia conoscenze nel campo della tecnologia antivirus o anti-spam.

Convenzioni del documento

Per facilitare l'individuazione e l'interpretazione delle informazioni, la documentazione di utilizza le convenzioni illustrate di seguito.

CONVENZIONE	DESCRIZIONE
TUTTO MAIUSCOLO	Acronimi, abbreviazioni e nomi di alcuni comandi e tasti della tastiera
Grassetto	Menu e comandi dei menu, pulsanti dei comandi, schede, opzioni e attività ScanMail
Corsivo	Riferimenti ad altri documenti
`Carattere a spaziatura fissa`	Esempi, righe di comando campione, codice del programma, nomi di file e output programmi
Nota:	Note sulla configurazione
Suggerimento:	Consigli
ATTENZIONE!	Promemoria per azioni o configurazioni da evitare

Capitolo 1

Introduzione a Trend Micro Hosted Email Security

Trend Micro™ Hosted Email Security garantisce alte prestazioni, servizi di protezione in hosting a prezzo competitivo e protezione aziendale da spam, virus e contenuti sconvenienti prima che raggiungano la rete.

Gli argomenti trattati nel presente capitolo includono:

Funzioni di Hosted Email Security

Hosted Email Security fornisce opzioni di gestione più complete, consentendo di personalizzare la protezione dalle minacce e di impostare criteri di utilizzo della posta elettronica in base alle esigenze dell'organizzazione.

- Filtro minacce personalizzato, filtro e-mail in uscita (opzionale)
- Funzionalità di filtraggio contenuto
- Crittografia e-mail (servizio separato, aggiuntivo, venduto separatamente)

Servizio aggiuntivo di crittografia e-mail

La crittografia e-mail Trend Micro per la posta in uscita è un servizio aggiuntivo di Hosted Email Security, disponibile per l'acquisto. La crittografia e-mail è completamente integrata con le funzionalità di filtraggio del contenuto di Hosted Email Security. Il servizio non esegue la crittografia e-mail automaticamente. Una volta abilitato, il servizio di crittografia e-mail appare come opzione di implementazione della regola all'interno della console di amministrazione Hosted Email Security. Sarà necessario configurare le regole che applicano la crittografia come azione di una regola. Per le direttive sulla creazione di regole che applicano la crittografia, consultare *Crittografa messaggio e-mail* a pagina 3-20.

Per utilizzare questo servizio di crittografia della posta, è necessario prima disporre di Hosted Email Security con filtraggio in uscita.

Hosted Email Security Flusso di messaggi

La *Figura 1-1* mostra il flusso di traffico di messaggi che proviene da Internet, attraversa i server Hosted Email Security e raggiunge il server di messaggistica.

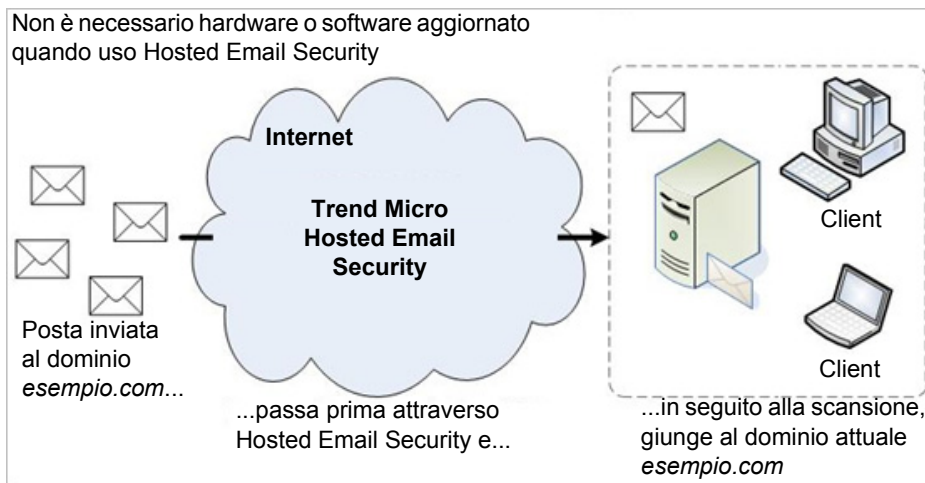



FIGURA 1-1 Hosted Email Security schema del flusso di lavoro

Hosted Email Security esegue i seguenti processi:

1. Il server di posta da cui provengono i messaggi esegue una ricerca DNS per determinare il percorso del dominio esempio.com. Il record Mail eXchange (MX) per esempio.com contiene l'indirizzo IP di Hosted Email Security invece dell'indirizzo IP originale per esempio.com, perché Hosted Email Security deve analizzare la posta aziendale prima della consegna finale al server di posta locale.
2. Il server di posta da cui provengono i messaggi indirizza la posta a Hosted Email Security.
3. I server Hosted Email Security accettano il messaggio, eseguono un filtraggio e applicano la corrispondenza di criteri per conto dell'utente.
4. Supponendo che il messaggio venga messo in coda per la consegna in base a criteri di sicurezza o allo stato di validità, i server Hosted Email Security indirizzano il messaggio ai server di posta esempio.com originali.

Livelli di protezione

Hosted Email Security offre due livelli di protezione che comprendono:

- Filtro a livello della connessione e-mail basato sulla reputazione
- Filtro e-mail basato sul contenuto

Filtro a livello della connessione e-mail basato sulla reputazione

Quando un server di posta a monte tenta di connettersi ai server Hosted Email Security, il server Hosted Email Security invia una query al server Email Reputation per determinare se l'indirizzo IP del mittente che si connette sia "affidabile". Hosted Email Security esegue questo primo livello di filtraggio prima di ricevere materialmente il messaggio; il contenuto del messaggio non viene quindi mai analizzato.

Se l'indirizzo IP di chi invia è considerato una fonte di spam, l'indirizzo IP del server che invia viene definito "non affidabile". Hosted Email Security rifiuta in modo permanente il tentativo di connessione da parte di questo indirizzo IP.

Se il computer del mittente fa parte di una botnet o di un PC zombie, l'indirizzo IP sarà inserito nel database ERS (Email Reputation Services) dinamico che identifica le fonti di spam man mano che emergono e finché sono attive. Hosted Email Security comunica al server che invia che Hosted Email Security è temporaneamente non disponibile. Se si tratta di un server legittimo, verrà effettuato un altro tentativo.

Filtro e-mail basato sul contenuto

Dopo che il messaggio passa attraverso il primo livello di protezione, Hosted Email Security applica il filtro del contenuto attraverso due motori di scansione:

- Spam e phishing
- Malware (virus, spyware e così via)

In questi motori di scansione sono integrate più tecnologie, ad esempio:

- File di pattern (o firme di spam)
- Regole euristiche
- Apprendimento macchina (o filtraggio statistico)
- Reputazione URL

Hosted Email Security esamina il contenuto del messaggio per determinare se il messaggio contiene malware come ad esempio virus, oppure se si tratta di spam e così via, in base ai criteri basati sul contenuto per questo messaggio.

Requisiti di sistema

Hosted Email Security non richiede altro hardware (se non il gateway di posta) nei locali. Tutto l'hardware di scansione si trova sui sicuri centri operativi di rete di Trend Micro. Per accedere all'account di amministrazione Hosted Email Security basato sul Web, è necessario un personal computer con accesso a Internet.

Software richiesto per l'accesso all'account

L'utilizzo della console Web Hosted Email Security richiede Java Script™ e Hosted Email Security supporta i seguenti browser per la console Web:

- Microsoft™ Internet Explorer™ 6.0 e 7.0
- Mozilla™ Firefox™ 2.0

Rete in sede

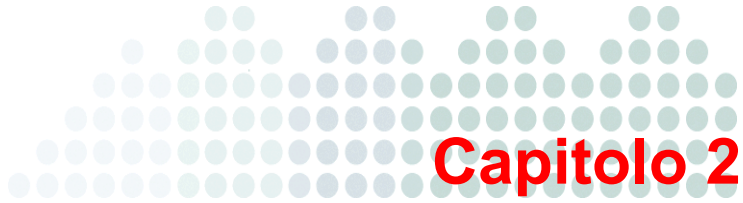
Prima di attivare Hosted Email Security, verificare la presenza di:

- Gateway Internet esistente o connessione SMTP al gruppo di lavoro
- Accesso al record di scambio posta DNS per il reindirizzamento del record host di posta MX. (Per ulteriori informazioni o assistenza nella configurazione, rivolgersi al proprio provider di servizi.)

Nota: Non reindirizzare il record MX finché non si riceve la conferma che l'account è stato creato. Se si reindirizza il record MX prima di aver impostato l'account, il messaggio e-mail andrà perso. Trend Micro fornisce tutti i dettagli per il reindirizzamento.

Impostazioni Hosted Email Security predefinite

Per garantire un servizio continuo e di elevata qualità, e per proteggere la rete da attacchi SMTP comuni quali inondazioni di posta e "Zip of Death", per impostazione predefinita le limitazioni del sistema di servizi comprendono le seguenti:

- Limiti di dimensione dei messaggi: 50 MB per messaggio
- Livelli totali integrati nei file compressi: 20 livelli
- Dimensione totale messaggio decompresso: 30 MB
- File totali nell'archivio compresso: 353 file
- Memorizzazione di quarantena totale per postazione: 50 MB
- Voci di mittenti approvati totali per postazione: 50

Capitolo 2

Utilizzo Hosted Email Security

Questo capitolo fornisce informazioni di base per l'accesso e l'uso della console di amministrazione Hosted Email Security e per la comprensione dei rapporti disponibili dalla console.

Gli argomenti trattati nel presente capitolo includono:

Informazioni preliminari

Per funzionare in modo corretto ed efficiente, Hosted Email Security deve essere configurato. La procedura di configurazione include i seguenti passaggi di base:

TABELLA 2-1. Checklist della configurazione Hosted Email Security

PASSAGGIO	PER ULTERIORI INFORMAZIONI	
1. Invio di informazioni sull'attivazione dell'account	*Invio di informazioni sull'attivazione dell'account* a pagina 2-3	❑
2. Accesso alla console di amministrazione basata sul Web	*Primo accesso* a pagina 2-10	❑
3. Aggiunta di uno o più domini all'account	*Gestione dei domini* a pagina 5-17	❑
4. Conferma del recapito posta mediante Hosted Email Security	*Conferma del recapito posta mediante il servizio* a pagina 5-20	❑
5. Reindirizzamento del record MX per il proprio dominio	*Reindirizzamento del record MX* a pagina 2-5	❑
6. Configurazione dell'agent MTA, se applicabile	*Configurazione di MTA (Mail Transfer Agent)* a pagina 2-6	❑

Registrazione e attivazione di Hosted Email Security

Per l'attivazione, occorrono un codice di attivazione (CA) o una chiave di registrazione (CR). Se non si dispone di un AC o una CR, contattare il proprio rappresentante di vendita Trend Micro. Non sarà possibile utilizzare Hosted Email Security fino a quando non viene immesso un codice di attivazione valido.

Per poter utilizzare il servizio, è necessario registrarlo. È possibile effettuare la registrazione online al seguente indirizzo:

https://olr.trendmicro.com/registration/eu/it/login.aspx

Il servizio di crittografia e-mail è un componente aggiuntivo di Hosted Email Security, pertanto deve essere acquistato separatamente.

Invio di informazioni sull'attivazione dell'account

Prima di utilizzare Hosted Email Security, è necessario attivare l'account.

Per attivare l'account Hosted Email Security:

1. Individuare la conferma di acquisto e la chiave di registrazione nel messaggio e-mail inviato da Trend Micro.
2. Per completare la procedura di registrazione, visitare il sito per la registrazione online di Trend Micro (URL contenuto nel messaggio e-mail), quindi selezionare un nome utente e una password.
3. Trend Micro invia un'e-mail con il nome utente selezionato e l'URL della console di amministrazione di Hosted Email Security.
4. Accedere alla console di amministrazione con il nome utente scelto. Verrà richiesto di inserire le informazioni relative al dominio e all'IP.
5. Fare clic su **Invia**. Trend Micro imposterà l'account dell'utente e invierà un messaggio e-mail di conferma. Questa operazione viene eseguita entro 24-48 ore. Il messaggio conterrà informazioni su dove indirizzare il record MX.
6. Inviare un messaggio e-mail di prova all'indirizzo e-mail di prova, per verificare che la posta possa passare attraverso Hosted Email Security.
7. Reindirizzare il record MX come illustrato nell'e-mail precedentemente citata.

Nota: Non reindirizzare il record MX finché non si riceve la conferma che l'account è stato creato. Se si reindirizza il record MX prima di aver impostato l'account, il messaggio e-mail andrà perso.

Ricezione della chiave di registrazione e del codice di attivazione

Chiave di registrazione

I clienti del Nord America, Europa, Medio Oriente e Africa necessitano di una chiave di registrazione (RK, Registration Key) per poter effettuare la registrazione di Hosted Email Security. Questa chiave è composta da 22 caratteri, compresi i trattini, e ha il seguente formato:

```
XX-XXXX-XXXX-XXXX-XXXX
```

I clienti nelle aree sopra riportate devono effettuare la registrazione di Hosted Email Security utilizzando la chiave di registrazione, prima di ricevere il codice di attivazione che consente di iniziare ad utilizzare il servizio.

Codice di attivazione

Il codice di attivazione è richiesto per tutti i clienti. La console Web visualizza lo stato della licenza. Il CA è composto da 37 caratteri (compresi i trattini) e ha il seguente formato:

```
XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Dopo aver registrato Hosted Email Security, Trend Micro invierà il codice di attivazione.

Attivazione del servizio Hosted Email Security

Quando si imposta Hosted Email Security per la prima volta, la prima schermata visualizzata è Attivazione del servizio, mostrata in *figura 2-1*. Utilizzare questa schermata per accedere ai domini da gestire tramite il servizio Hosted Email Security.

Nota: Per applicare le impostazioni di reputazione IP alla posta in arrivo, Hosted Email Security deve disporre dell'elenco dei domini dell'azienda.

Per aggiungere un dominio da gestire tramite Hosted Email Security:

1. Inserire le seguenti informazioni nei campi forniti (i campi obbligatori sono mostrati in grassetto):
    - Nuovo **nome dominio**
    - **Indirizzo IP o FQDN** (Fully Qualified Domain Name)
    - **Numero porta** del relativo server di posta
    - Numero di **postazioni assegnate** a questo dominio
    - Account e-mail di prova (Utilizzare questo indirizzo e-mail come destinatario dei messaggi di prova per confermarne il recapito mediante Hosted Email Security.)
2. Selezionare **Attivazione filtro posta in uscita**, quindi fornire l'indirizzo IP dei server posta in uscita di destinazione.
3. Fare clic su **Attiva dominio.** Il dominio viene visualizzato nella tabella Domini nella parte inferiore della schermata.

4. Fare clic su **Invia**. Se il dominio è valido ed esiste un record MX per il dominio, vengono visualizzati il nuovo dominio, l'indirizzo IP o l'FQDN, il numero porta, le postazioni e altre informazioni nella tabella Domini sulla parte inferiore della schermata e Trend Micro invia un'e-mail di "benvenuto" all'indirizzo e-mail di amministrazione nel record.

Attivazione del servizio

Per utilizzare Hosted Email Security, è necessario fornire le seguenti informazioni.

Per aggiungere un dominio, sono necessarie le seguenti informazioni.

Nota: dopo l'attivazione del dominio, l'utente riceve un messaggio di posta elettronica di benvenuto, contenente le istruzioni necessarie all'aggiornamento dei record MX del dominio piena funzionalità di Trend Micro Hosted Email Security, finché il record MX non punterà a Hosted Email Security Inbound MTA.

Aggiunta di un dominio

Nome di dominio*: (ad es.: esempio.com)

Postazione assegnata *: di 10 postazioni rimanenti

Server di destinazione*: Indirizzo IP o FQDN | Preferenza

Numero di porta *: 25

Attivazione filtro posta in uscita

Avviso: se si attiva il filtro della posta in uscita senza specificare i server di posta in uscita si bloccherà tutto il traffico in uscita instradato attraverso il servizio.

Server posta in uscita: Indirizzo IP

Per i domini aggiunti prima del [2013-02-23], è possibile che non siano elencati tutti i server di posta in uscita associati a questi domini. Tuttavia, Hosted Email Security garantisce che il traffico proveniente dai server non inclusi nell'elenco siano ricevuti ed elaborati correttamente. L'utente può scegliere di aggiungere i server all'elenco **Server posta in uscita**.

Destinatario e-mail di prova: @<nome dominio>

Aggiungi dominio

FIGURA 2-1. Schermata di Attivazione del servizio

Reindirizzamento del record MX

Il record Mail eXchange (MX) determina l'indirizzamento del messaggio per tutti i messaggi e-mail inviati al dominio dell'utente. Per indirizzare i messaggi destinati al dominio nel sistema Hosted Email Security, è necessario reindirizzare il record MX. L'e-mail di benvenuto ricevuta illustra dove reindirizzare il record MX.

Per reindirizzare il record MX, modificare il record attuale con quello fornito nell'e-mail di benvenuto inviata da Trend Micro dopo la registrazione. La modifica può essere eseguita manualmente (tipica per piccoli account autogestiti) o da un tecnico dell'assistenza.

Se si è incerti sulla modalità di configurazione dei record MX del dominio, rivolgersi al proprio provider Internet o al tecnico del Domain Name Service (DNS).

Nota: La propagazione DNS può richiedere fino a 48 ore. In questo lasso di tempo, non interrompere la protezione in sede. È possibile che l'utente riceva direttamente qualche messaggio e-mail per un breve periodo di tempo, finché la transizione non è terminata.

Configurazione di MTA (Mail Transfer Agent)

Per tutti i utenti di Hosted Email Security, tutti i messaggi "spam o phishing" inizialmente vengono eliminati per impostazione predefinita. Se si dispone della versione completa, è possibile modificare questa regola. Consultare *Modifica di una regola esistente* a pagina 3-35.

L'utente può decidere di configurare l'agente MTA in modo che gestisca lo spam in accordo con i criteri di sicurezza aziendali. I messaggi contrassegnati possono essere inoltrati a una cartella di spam, eliminati, passati all'utente finale, e così via. Se si sceglie di contrassegnare questi messaggi, la riga dell'oggetto dei messaggi di spam sarà contrassegnata con **Spam/Phishing>** anteposto alla riga di oggetto originale.

Nota: Questa documentazione non si prefigge di fornire istruzioni dettagliate sulla configurazione dell'agent MTA. Se è necessaria assistenza, contattare l'amministratore di sistema.

Attivazione filtro per la posta in uscita

La crittografia e-mail di Trend Micro è disponibile solo come servizio aggiuntivo per Hosted Email Security con filtro della posta in uscita. Il filtro della posta in uscita è disponibile, senza costi aggiuntivi.

Se non si dispone di un account ORL (Online Registration) Trend Micro, per attivare questa funzione è necessario contattare l'assistenza tecnica Trend Micro. Con un account OLR è possibile eseguire questa operazione dall'interno della console di amministrazione Hosted Email Security.

Se si dispone di un account OLR

Se si dispone di un account della registrazione in linea (OLR), l'attivazione del filtro della posta in uscita è un'operazione semplice.

Per attivare il filtro della posta in uscita:

1. Dal menu a sinistra selezionare **Amministrazione > Gestione dominio** per aprire la schermata Gestione dominio.
2. Nella tabella Domini nella parte inferiore della schermata, fare clic sul nome di dominio con collegamento ipertestuale per attivare il filtro della posta in uscita. Viene visualizzata la schermata **Gestione dominio > {proprio-nome-dominio}**, i cui campi sono popolati con le informazioni sul record relativo a quel dominio.
3. Selezionare **Attivazione filtro posta in uscita**.
4. Specificare almeno un **server posta in uscita** utilizzando il suo indirizzo IP.
5. Fare clic su **Salva**. Hosted Email Security avvia la procedura di attivazione del filtro della posta in uscita per quel dominio e lo stato del dominio indica la "modifica in corso".

Suggerimento: Dopo aver fatto clic su **Salva**, viene avviata la procedura di attivazione. Per il completamento della procedura sono necessarie 2 ore. Una volta completata, Hosted Email Security cambia lo stato del dominio da "modifica in corso" a "Attivato".

Se non si dispone di un account OLR

Il filtro di posta in uscita è una funzione la cui configurazione richiede interazione con lo staff di Trend Micro. Se il filtro della posta in uscita è stato configurato per l'account personale, la propria azienda riceverà un messaggio e-mail di conferma da Trend Micro indicante che questa funzione è stata abilitata e il server da utilizzare per l'accesso.

Prima di contattare l'assistenza tecnica Trend Micro per l'attivazione del filtro per la posta in uscita, è necessario fornire le informazioni indicate:

- Nome account
- Nome dominio e indirizzo e-mail valido per quel dominio
- Nome
- Indirizzo e-mail
- Indirizzo IP del server di posta in uscita

L'assistenza tecnica Trend Micro apporterà tutte le modifiche necessarie per applicare il filtro Hosted Email Security alla posta in uscita e invierà una notifica via e-mail ad attivazione avvenuta. L'utente riceverà inoltre ulteriori istruzioni su come indirizzare la posta in uscita ai server Hosted Email Security.

Per ulteriori informazioni sull'attivazione del filtro per la posta in uscita o per richiedere il servizio di filtro per la posta in uscita, contattare l'assistenza tecnica Trend Micro.

Verifica filtro per la posta in uscita

In seguito all'attivazione del filtro per la posta in uscita da parte dell'assistenza Trend Micro, verrà inviato un messaggio e-mail di notifica. Selezionare **Amministrazione > Gestione dominio** per verificare che il filtro della posta in uscita sia abilitato, come mostrato in *Figura 2-2* a pagina 2-9.

FIGURA 2-2. Schermata Gestione dominio che mostra che "Filtro posta in uscita" è attivato

Acquisto della crittografia e-mail

Per acquistare il servizio di crittografia e-mail, è necessario aver acquistato Hosted Email Security con il filtro della posta in uscita. È possibile effettuare una prova gratuita della crittografia e-mail mentre si è nel periodo di prova di Hosted Email Security, ma non è possibile acquistare la crittografia e-mail fino a quando non si effettua l'acquisto di Hosted Email Security e si dispone del filtro della posta in uscita.

Nota: In alcuni paesi, è necessario ottenere una chiave di registrazione (CR) prima di ottenere un Codice di attivazione (CA). Se si dispone di una CR ma non si dispone ancora di un CA, eseguire la registrazione online dal sito di registrazione online di Trend Micro per richiedere il codice: https://olr.trendmicro.com/registration

---

Disattivazione Hosted Email Security

Per disabilitare Hosted Email Security, è necessario seguire la stessa procedura utilizzata per l'inizializzazione del servizio, quindi reindirizzare il record MX affinché indirizzi tutto il traffico SMTP in entrata al server di posta dell'utente. Consultare *Reindirizzamento del record MX* a pagina 2-5.

Accesso alla console di amministrazione

È possibile visualizzare rapporti e utilizzare lo strumento di verifica posta per individuare i messaggi, accedendo alla console Web di Hosted Email Security. Come utente di Hosted Email Security (versione completa), è possibile effettuare modifiche ai criteri di sicurezza per i messaggi.

Primo accesso

Il pacchetto di benvenuto che l'utente riceve dopo l'acquisto di Hosted Email Security contiene un nome utente e una password da utilizzare durante l'accesso iniziale.

Per accedere alla console:

1. Per passare alla pagina di accesso, inserire nel browser l'URL presente nel messaggio di conferma ricevuto (vedere *Passaggio 2* a pagina 2-3).

FIGURA 2-3. Schermata di accesso Hosted Email Security

2. Se si dispone di un account ORL Trend Micro, selezionare **Accedere con il nome utente e la password della registrazione in linea di Trend Micro.**
3. Inserire il **nome utente** e la **password**.
4. Fare clic su **Accedi**.

Suggerimento: Dopo il primo accesso, Trend Micro consiglia di modificare la password per garantire la sicurezza dell'account Hosted Email Security. Consultare *Amministrazione* a pagina 5-11.

Uso della console Web di Hosted Email Security

La console Web di Hosted Email Security agli amministratori e-mail di creare rapporti, visualizzare registri, eseguire attività di amministrazione e impostare o modificare criteri.

Per informazioni dettagliate sull'uso della console Web di Hosted Email Security, consultare i file della Guida in linea. Per accedere alla Guida in linea completa, fare clic su "Sommario e indice" nel menu a discesa della Guida oppure passare a una schermata specifica facendo clic sul punto interrogativo blu ( ) nell'angolo in alto a destra di ogni schermata.

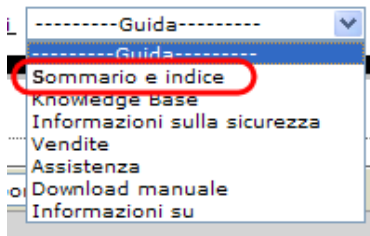



FIGURA 2-4. Menu a discesa della Guida

Rapporti

La schermata Pannello di controllo (*figura 2-5*) viene visualizzata quando si accede a Hosted Email Security. *Tabella 2-2* a pagina 2-14 descrive i grafici del pannello di controllo.

Gli utenti di Hosted Email Security possono creare query nella posta in entrata o nella posta in uscita. Selezionare **In entrata** o **In uscita** dall'elenco a discesa "Direzione traffico e-mail".

Per le specifiche relative alle azioni Hosted Email Security, fare clic sulla scheda appropriata o doppio clic sull'immagine nella schermata del pannello di controllo.

FIGURA 2-5. Schermata Rapporto riepilogativo (traffico in entrata)

Tabella 2-2 a pagina 2-14 descrive i grafici della schermata della scheda Pannello di controllo.

TABELLA 2-2. Grafici della schermata del pannello di controllo

NOME GRAFICO	NOME SCHEDA	DESCRIZIONE
Traffico totale	Traffico	Mostra tutto il traffico e-mail bloccato e accettato per il dominio selezionato.
Dimensioni accettate	Dimensione	Mostra le dimensioni totali (in KB) del traffico e-mail accettato per il dominio selezionato.
Riepilogo minacce	Minacce	Mostra la percentuale degli specifici tipi di messaggi che compongono il traffico e-mail per il dominio di posta selezionato.
Dettagli minacce	Dettagli	Mostra la distribuzione dettagliata del traffico e-mail per il dominio di posta selezionato.[*]
Destinatari principali dello spam Principali mittenti di spam	Destinatari principali spam	Mostra i destinatari principali del messaggio di spam (o i mittenti, per la posta in uscita) per il dominio di posta selezionato
Destinatari principali dei virus Principali mittenti di virus	Destinatari principali virus	Mostra i destinatari principali del virus (o i mittenti, per la posta in uscita) per il dominio di posta selezionato

*. Per evitare ingombri, nella visualizzazione del pannello di controllo di questo rapporto non è presente la legenda.

Scheda Traffico

Fare clic sulla scheda **Traffico** per visualizzare la schermata Traffico totale (*figura 2-6*), che mostra tutto il traffico e-mail bloccato e accettato per il dominio selezionato a ogni intervallo e la tendenza del traffico per il periodo selezionato. La legenda indica il numero di messaggi e-mail bloccati, di messaggi e-mail accettati per ulteriore elaborazione, la percentuale di traffico bloccato e il numero totale di messaggi e-mail per il dominio selezionato. Per una maggiore visibilità, la scala della percentuale bloccata è posta nella parte destra del grafico.

Nota: Il traffico "bloccato" ha significati differenti per il traffico in entrata e per quello in uscita. Il traffico in entrata viene filtrato da Trend Micro Email Reputation Services, a differenza di quello in uscita. Se i messaggi in uscita vengono bloccati, questo non dipende dalla reputazione dei messaggi e-mail, ma da problemi con il servizio di posta relay di Hosted Email Security, come illustrato in seguito.

Per la posta in entrata:

- **Bloccato:** i numero di tentativi di messaggi dannosi da inviare al dominio selezionato. Questo traffico di messaggi dannosi è rappresentato dalle connessioni bloccate dal filtro Trend Micro Email Reputation Services (ERS).
- **Accettato:** i numero di messaggi che superano il filtro ERS e vengono accettati per ulteriore elaborazione da Trend Micro Hosted Email Security.
- **% bloccata:** l percentuale di traffico di messaggi bloccato da ERS per il dominio di posta selezionato.
- **Totale:** i numero totale di messaggi e-mail elaborati da Hosted Email Security per il dominio di posta selezionato. È la somma di traffico bloccato e accettato.

Solo per la posta in uscita:

- **Bloccati:** i numero dei tentativi del messaggio rifiutati dal server di posta relay di Hosted Email Security. I motivi del blocco sono i seguenti.
  - Impossibilità di risolvere l'indirizzo del destinatario ("`utente@???.com`").
  - Indirizzo del mittente contraffatto dallo spammer in modo che il messaggio sembri provenire dal dominio del cliente.
  - Il server di posta dell'utente è compromesso (ad esempio un relay aperto) e sta inviando messaggi spam.

Nota: I messaggi in uscita non vengono bloccati dal filtro Trend Micro Email Reputation Services (ERS), ma dal servizio di posta relay di Hosted Email Security.

- **Accettato:** i numero di messaggi accettati per ulteriore elaborazione da Trend Micro Hosted Email Security.
- **% bloccata:** l percentuale di traffico di messaggi bloccato dal servizio di posta relay di Hosted Email Security per il dominio di posta selezionato.
- **Totale:** i numero totale di messaggi e-mail elaborati da Hosted Email Security per il dominio di posta selezionato. È la somma di traffico bloccato e accettato.

FIGURA 2-6. Schermata Rapporto Traffico totale (traffico in entrata)

Scheda Dimensioni

Fare clic sulla scheda **Dimensioni** per visualizzare il rapporto Dimensioni accettate (*figura 2-7*), che mostra le dimensioni totali (in KB) del traffico e-mail accettato per il dominio selezionato. Il periodo predefinito inserito nei rapporti è *oggi* (giorno corrente). Le legenda indica le dimensioni totali dei messaggi non in quarantena, di quelli in quarantena e di quelli accettati. In questa scheda viene visualizzato un grafico per il traffico in entrata o in uscita, a seconda della direzione del traffico selezionata.

Non in quarantena: le dimensioni dei messaggi accettati che non sono stati messi in quarantena per il dominio di posta selezionato.

In quarantena: le dimensioni dei messaggi in quarantena per il dominio di posta selezionato. Se la quarantena non è stata configurata per i criteri di questo dominio di posta, non ci sarà posta in quarantena in questo grafico.

Dimensioni totali: le dimensioni totali dei messaggi accettati per il dominio di posta selezionato. È la somma di messaggi non in quarantena e in quarantena.

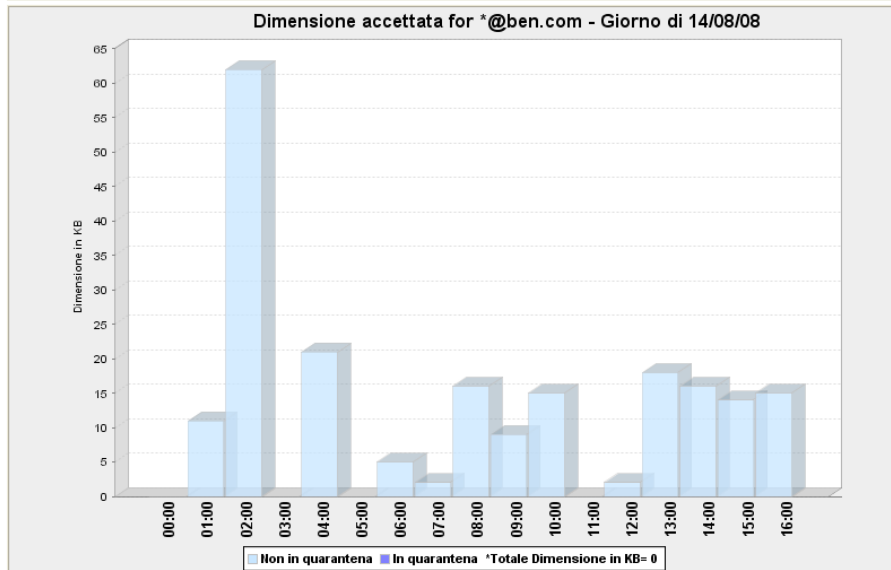



FIGURA 2-7. Schermata Rapporto Dimensioni accettate (traffico in entrata)

Scheda Minacce

Fare clic sulla scheda **Minacce** per visualizzare il rapporto Riepilogo minacce (*figura 2-8*), che mostra le condivisioni dei messaggi per tipo relativamente al dominio selezionato. Il periodo predefinito inserito nei rapporti è la settimana corrente. Il grafico a torta mostra la percentuale dei vari tipi di messaggi per il dominio selezionato.

La legenda indica il numero di messaggi e-mail bloccati, i messaggi sicuri, i messaggi e-mail di phishing, spam e virus, nonché il numero totale di messaggi per il dominio di posta selezionato.

- **Bloccati:** pr il dominio di posta selezionato, il numero delle connessioni di posta bloccate da Trend Micro ERS (per la posta in entrata) o dal servizio di posta relay di Trend Micro Hosted Email Security (per la posta in uscita).
- **Sicuri:** pr il dominio di posta selezionato, il numero di messaggi e-mail considerati sicuri da Hosted Email Security.
- **Phishing:** pr il dominio di posta selezionato, il numero di messaggi e-mail identificati da Hosted Email Security come messaggi di phishing.
- **Spam:** pr il dominio di posta selezionato, il numero di messaggi e-mail identificati come messaggi di spam dal motore di prevenzione euristica dello spam di Hosted Email Security.
- **Virus:** pr il dominio di posta selezionato, il numero di messaggi e-mail identificati da Hosted Email Security come messaggi contenenti un virus.
- **Altri:** pr il dominio di posta selezionato, il numero di messaggi e-mail filtrati da altri filtri dei contenuti Hosted Email Security (ad esempio il filtro per le dimensioni degli allegati).
- **Totale:** i numero totale di messaggi e-mail per il dominio di posta selezionato. È la somma di tutte e sei le categorie.

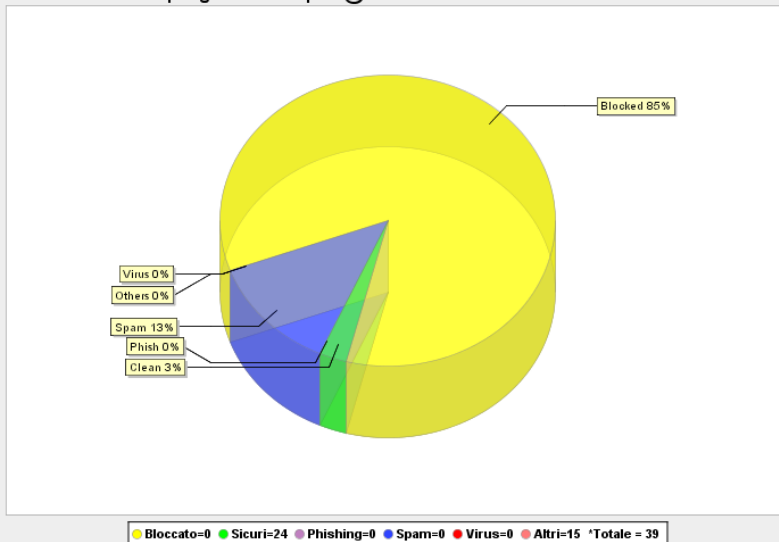



FIGURA 2-8. Schermata rapporto Riepilogo minacce (traffico in entrata)

Scheda Dettagli

Fare clic sulla scheda **Dettagli** per visualizzare il rapporto Dettagli minacce (*figura 2-13*), che mostra la distribuzione dettagliata del traffico e-mail per il dominio di posta selezionato. Il periodo predefinito inserito nei rapporti è la settimana corrente. Questo rapporto utilizza lo stesso schema colore degli altri. Vi sono tre grafici dettagliati e una tabella dei totali:

Grafico 1: numero di messaggi e percentuale di traffico bloccato, come mostrato in *figura 2-9*.

Nota: Il traffico "bloccato" ha significati differenti per il traffico in entrata e per quello in uscita, come spiegato in dettaglio in *Scheda Traffico* a partire da pagina 2-14.

Il grafico è simile al rapporto "Traffico totale" descritto in precedenza. Suddivide ulteriormente i messaggi accettati in varie categorie, ad esempio virus, phishing, spam, disinfetta e altri.

- L'asse verticale sulla sinistra corrisponde alle barre verticali, che indicano il numero totale di messaggi per il dominio di posta selezionato. Ogni barra verticale è composta dai valori relativi a messaggi bloccati, sicuri, con phishing, spam, virus e altro.
- L'asse verticale sulla destra corrisponde al grafico lineare, che rappresenta la percentuale di tutto il traffico bloccato da Trend Micro Email Reputation Services (ERS) ad ogni intervallo.

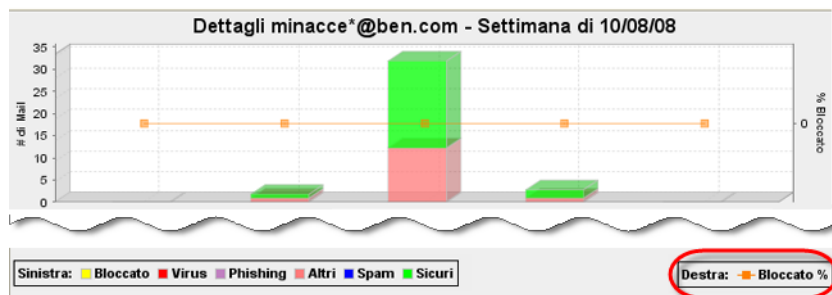



FIGURA 2-9. Rapporto Dettagli minacce, grafico 1 (traffico in entrata)

Grafico 2: numero di ogni tipo di messaggi e-mail: solo "spam" e "sicuri"

Ogni riga rappresenta il numero di un tipo di e-mail ad ogni intervallo, come mostrato in *figura 2-10*.

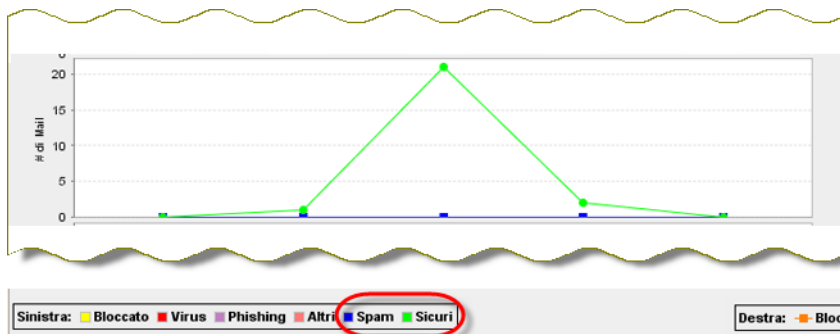



FIGURA 2-10. Rapporto Dettagli minacce, grafico 2 (traffico in entrata)

Grafico 3: numero di ogni tipo di minaccia e-mail: solo "virus," "phishing" e "altri"

Ogni riga rappresenta il numero di un tipo di minaccia e-mail ad ogni intervallo, come mostrato in *figura 2-11*.

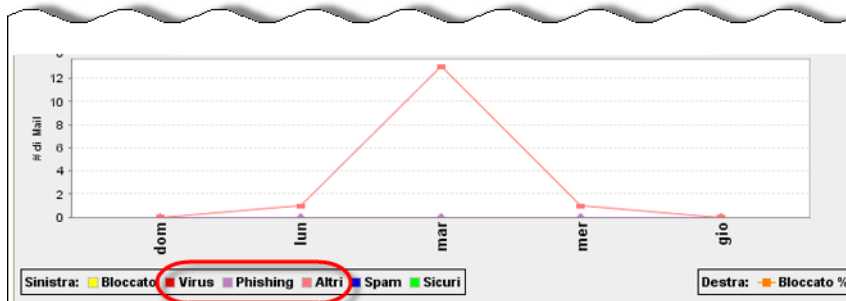



FIGURA 2-11. Rapporto Dettagli minaccia, grafico 3

Tabella dei totali: ogni settimana mostra il totale di:

- Percentuale di messaggi bloccati
- Numero di messaggi bloccati
- Numero di virus
- Numero di phishing
- Numero di spam
- Numero di messaggi disinfettati
- Altri
- Totale giornaliero

Settimanale Totali

Data	% Bloccato	# Bloccato	# Virus	# Phishing	# Spam	# Sicuri	# Altri	Totale
10-ago-2008	0	0	0	0	0	0	0	0
11-ago-2008	0	0	0	0	0	1	1	2
12-ago-2008	0	0	0	0	0	21	13	34
13-ago-2008	0	0	0	0	0	2	1	3
14-ago-2008	0	0	0	0	0	0	0	0
Totale	*0*	*0*	*0*	*0*	*0*	*24*	*15*	*39*

FIGURA 2-12. Rapporto Dettagli minacce, tabella totali

Nota: Per evitare ingombri, nella visualizzazione del pannello di controllo di questo rapporto non è presente la legenda.

Settimanale Totali

Data	% Bloccato	# Bloccato	# Virus	# Phishing	# Spam	# Sicuri	# Altri	Totale
10-ago-2008	0	0	0	0	0	0	0	0
11-ago-2008	0	0	0	0	0	1	1	2
12-ago-2008	0	0	0	0	0	21	13	34
13-ago-2008	0	0	0	0	0	2	1	3
14-ago-2008	0	0	0	0	0	0	0	0
Totale	*0*	*0*	*0*	*0*	*0*	*24*	*15*	*39*

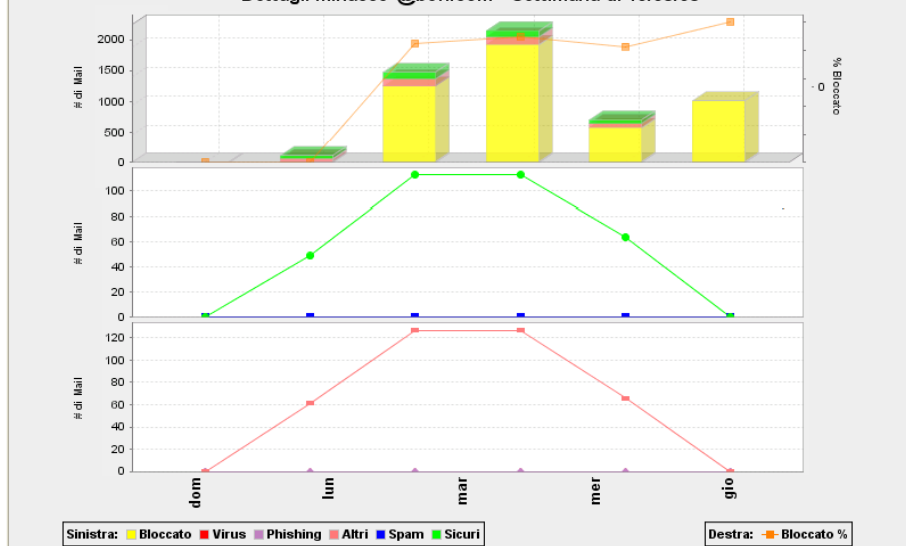
FIGURA 2-13. Schermata rapporto Dettagli minacce (traffico in entrata)

Data	% Bloccato	# Bloccato	# Virus	# Phishing	# Spam	# Sicuri	# Altri	Totale
12-ago-2009	0	0	0	0	0	0	0	0
13-ago-2009	0	0	0	0	0	49	61	110
14-ago-2009	84.7	1,328	0	0	0	113	127	1,568
15-ago-2009	89.5	2,050	0	0	0	113	127	2,290
16-ago-2009	82.6	617	0	0	0	64	66	747
17-ago-2009	100	1,072	0	0	0	0	0	1,072
Total	*87.6*	*5,067*	*0*	*0*	*0*	*339*	*381*	*5,787*

FIGURA 2-14. Schermata rapporto Dettagli minacce (traffico in uscita)

Scheda Destinatari principali dello spam

Fare clic sulla scheda **Spam più pericoloso** per visualizzare il rapporto Destinatari principali dello spam (*figura 2-15*) o Mittenti principali dello spam, che mostra i destinatari o i mittenti principali dello spam per il dominio di posta selezionato, a seconda della direzione del traffico di posta selezionata. Il periodo predefinito inserito nei rapporti è la *settimana corrente*. I rapporti Destinatari principali dello spam vengono visualizzati con il fuso orario di Greenwich.

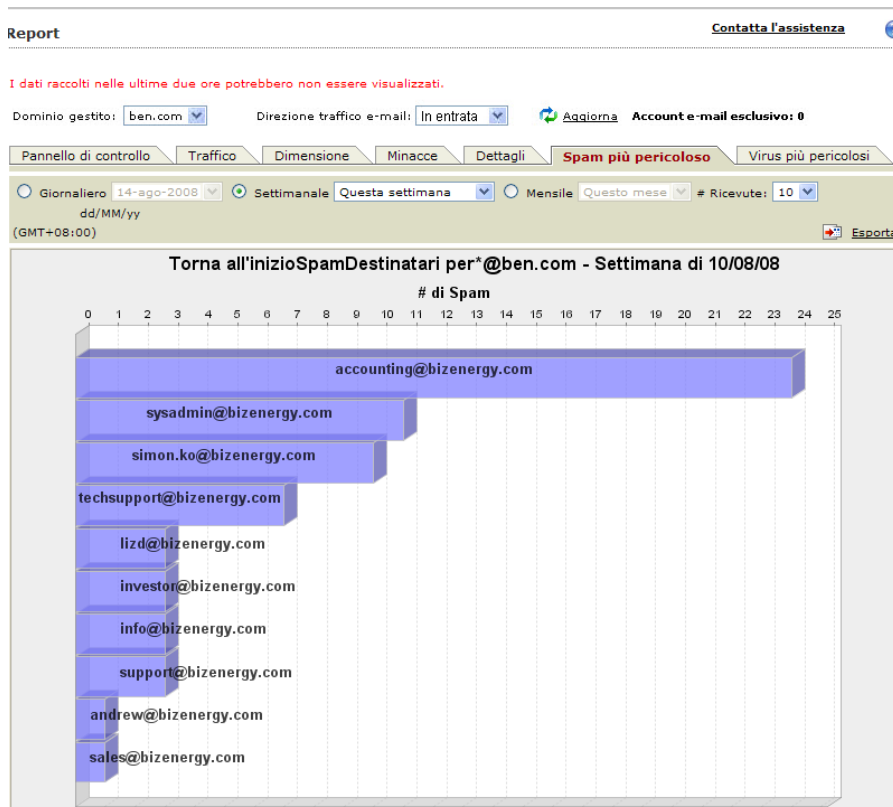



FIGURA 2-15. Schermata rapporto Destinatari principali dello spam (traffico in entrata)

Scheda Destinatari principali dei virus

Fare clic sulla scheda **Virus più pericolosi** per visualizzare rapporto Destinatari principali dei virus (*figura 2-16*) o Mittenti principali dei virus per il dominio di posta selezionato. Selezionare "in entrata" dal menu a discesa della direzione traffico e-mail per visualizzare il rapporto dei destinatari e "in uscita" per il rapporto dei mittenti. Il periodo predefinito inserito nei rapporti è la *settimana corrente*. I rapporti destinatari/mittenti principali dei virus vengono visualizzati con il fuso orario di Greenwich.

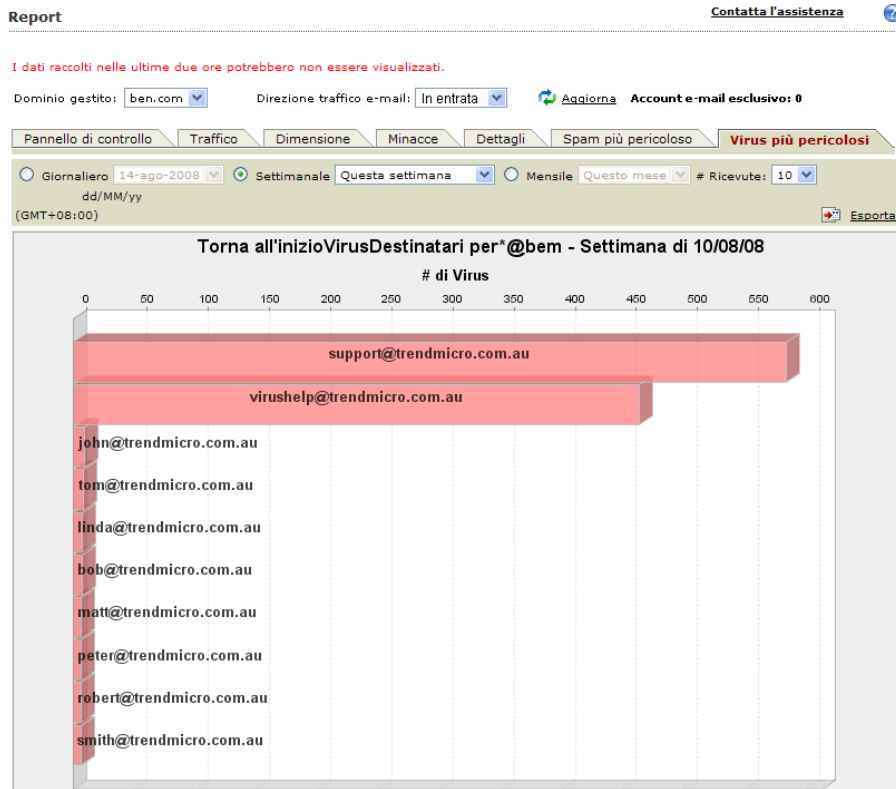
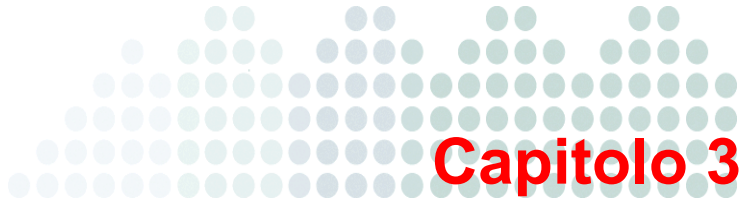



FIGURA 2-16. Schermata rapporto Destinatari principali dei virus (traffico in entrata)

Capitolo 3

Gestione dei criteri

Questo capitolo fornisce informazioni per la creazione e la gestione dei criteri di scansione utilizzando la console di amministrazione di Hosted Email Security.

Gli argomenti trattati nel presente capitolo includono:

Panoramica dei criteri

Un criterio Hosted Email Security è un insieme di regole per un dominio di posta specifico. Possono esistere varie regole per ogni dominio o criterio di dominio, ma ogni dominio può avere un solo criterio.

Gli amministratori possono vedere in qualsiasi momento le regole che si applicano alla loro organizzazione.

In base al livello di servizio, è possibile visualizzare, modificare e creare regole per criteri di dominio specifici.

Versione completa: i utenti di questo livello di servizio hanno diritti di creazione e modifica.

FIGURA 3-1. Schermata Criterio, versione completa

La schermata Criterio mostra un elenco delle regole definite e del relativo stato. Se il livello di servizio lo consente, in questa schermata è possibile aggiungere una nuova regola e modificare, copiare o eliminare regole esistenti. Per una descrizione delle regole predefinite, vedere *Impostazioni dei criteri predefiniti* a pagina 3-3.

Nella parte superiore destra dell'elenco regole, vengono mostrati il numero di regole visualizzato nella pagina e il numero totale di regole. È possibile applicare filtri all'elenco utilizzando le caselle a discesa in alto.

Le regole vengono visualizzate in una tabella e ordinate in base alla sequenza di applicazione durante l'analisi di Hosted Email Security. I contenuti di ogni tabella possono essere ordinati facendo clic sull'intestazione di una colonna. Ad esempio, per riordinare la tabella in ordine alfabetico per azione, fare clic sull'intestazione della colonna Azione. Fare clic sull'intestazione della colonna Timestamp per filtrare le regole in base alla data dell'ultima modifica. In alternativa, fare clic su Ultimo utilizzo per visualizzare le regole dell'ultimo timestamp utilizzato. Se la regola non è stata attivata, il valore in questa colonna sarà *Mai*.

TABELLA 3-1. Icone abilitate e disabilitate

ICONA	DESCRIZIONE
	La regola è abilitata.
	La regola è disabilitata.

Fare clic sull'icona a destra di ogni regola per abilitare o disabilitare la regola.

Nota: La disabilitazione di una regola può avere effetti negativi sulla sicurezza e-mail. Ad esempio, se si disabilita una regola antivirus, si può essere esposti ad attacchi virali.

Impostazioni dei criteri predefiniti

Le regole seguenti costituiscono i criteri predefiniti per tutti i utenti di Hosted Email Security.

I utenti di Hosted Email Security possono modificare le regole predefinite e creare nuove regole.

Regola 1: Virus

Se viene rilevato uno dei seguenti elementi, viene eliminato tutto il messaggio.

a. Invio di posta in massa: progettato per la protezione dai virus spesso diffusi attraverso campagne di invii di posta in massa. Viene stabilito se un messaggio contiene un virus non disinfettabile e se mostra un comportamento simile ai messaggi diffusi con invii di posta in massa.

b. Virus non disinfettabile: viene stabilito se un messaggio contiene un virus non disinfettabile.

c. Virus disinfettabile: viene stabilito se un messaggio contiene un virus disinfettabile.

Regola 2: dimensioni del messaggio o numero di destinatari eccessivi

Questa regola è stata messa a punto per proteggere il sistema da attacchi Denial of Service (DOS) e Zip of Death. Il messaggio in entrata viene eliminato e Hosted Email Security invia al mittente una notifica se le rispettive dimensioni superano il limite predefinito di 50 MB o se è stato inviato a più di 50 destinatari. I utenti di Hosted Email Security possono modificare questa regola fino a un limite di sistema di 100 destinatari.

Regola 3: spam o phishing

Questa regola è stata ideata per rilevare i messaggi e-mail di spam o phishing. L'azione predefinita è l'eliminazione dei messaggi identificati come spam o phishing. Tutti i utenti di Hosted Email Security hanno la possibilità di modificare l'azione predefinita. Si consiglia di selezionare solo le azioni Elimina o Quarantena per questa regola. Tutti i messaggi e-mail in quarantena vengono salvati nella quarantena Hosted Email Security accessibile via Web per 21 giorni nella regione EMEA e 15 giorni in tutti gli altri paesi.

I utenti di Hosted Email Security avanzati possono modificare i parametri utilizzati per il tasso di intercettazione spam da Minimo (meno aggressivo) a Massimo (più aggressivo). L'impostazione predefinita è Moderatamente basso.

Nota: Esistono due regole predefinite relative allo spam. Per le newsletter o i messaggi e-mail simili a spam, fare riferimento alla regola: *Regola 5: newsletter o messaggi e-mail simili a spam*.

Regola 4: allegati ad alto rischio

Questa regola è disponibile solo per i utenti di Hosted Email Security. La regola elimina gli allegati ad alto rischio dai messaggi e-mail secondo le definizioni dei parametri della regola. Un esempio di allegato ad alto rischio potrebbe essere un file eseguibile con estensione .exe o un file multimediale (.mp3) rinominato file_innocuo.txt. Se si ritiene che un messaggio contenga un allegato ad alto rischio, l'allegato viene eliminato dal messaggio e-mail prima della consegna.

Regola 5: newsletter o messaggi e-mail simili a spam

Questa regola rileva la "gray-mail", ad esempio le newsletter. L'azione predefinita per questi messaggi simili a spam è Contrassegna oggetto (con "Spam>"). Si consiglia di selezionare solo le azioni Contrassegna oggetto o Quarantena per questa regola. Tutti i messaggi e-mail in quarantena vengono salvati nella quarantena Hosted Email Security accessibile via Web per 21 giorni nella regione EMEA e 15 giorni in tutti gli altri paesi.

I utenti di Hosted Email Security avanzati possono modificare i parametri utilizzati per il tasso di intercettazione spam da Minimo (meno aggressivo) a Massimo (più aggressivo). L'impostazione predefinita è Moderatamente alto.

Nota: Esistono due regole predefinite relative allo spam. Per i messaggi che molto probabilmente contengono spam o phishing, fare riferimento alla regola *Regola 3: spam o phishing*.

Regola 6: allegati con file compressi protetti da password

Questa regola consente agli utenti della versione completa di configurare l'azione da compiere in modo da gestire i messaggi e-mail con allegati contenenti file zip protetti da password. Per impostazione predefinita, i messaggi con allegati con file zip protetti da password vengono recapitati al destinatario e nel corpo del messaggio viene inserita una notifica che comunica la mancata scansione del file dell'allegato.

Criteri predefiniti di filtraggio della posta in uscita

Per tutti gli utenti Hosted Email Security, vengono aggiunte altre quattro regole predefinite. Queste regole sono progettate allo stesso modo delle omonime regole sopra descritte, ma si applicano solo alla posta in uscita. Le regole di filtraggio della posta in uscita sono:

- Posta in uscita – Virus
- Posta in uscita – Allegato ad alto rischio
- Posta in uscita – Dimensioni del messaggio o numero di destinatari eccessivi
- Posta in uscita – Spam o phishing

Filtro dei contenuti

Gli utenti di Hosted Email Security possono applicare le regole di filtraggio dei contenuti ai messaggi e-mail. Hosted Email Security fornisce opzioni di filtraggio dei contenuti flessibili e di facile utilizzo, che consentono di contrassegnare virtualmente qualsiasi tipo di contenuto.

Filtraggio del contenuto con le parole chiave

È possibile configurare le regole Hosted Email Security in modo che effettuino la corrispondenza con il contenuto come parte della logica di funzionamento. Hosted Email Security può effettuare la corrispondenza con il contenuto attraverso l’utilizzo di parole chiave, di espressioni regolari o di entrambe. Configurare il filtro del contenuto nel passaggio 2, al momento dell’aggiunta o della modifica di una nuova regola nel seguente modo.

Per configurare il filtro dei contenuti utilizzando le parole chiave, effettuare quanto segue:

1. Quando si aggiunge o si modifica una regola nel passaggio 2: In Seleziona parametri di scansione, selezionare **Avanzati.** Vengono visualizzate alcune opzioni, come quelle mostrate nella *figura 3-2* sotto riportata.

FIGURA 3-2. Opzioni di filtraggio dei contenuti

2. Selezionare la parte dell'e-mail di cui eseguire la scansione del contenuto. Le opzioni principali sono:
   - Oggetto
   - Corpo
   - Intestazione specificata
   - Allegato
3. Fare clic sul collegamento **parole chiave** a destra della selezione effettuata. Viene visualizzata la schermata Parole chiave, come mostrato nella *figura 3-3* sotto riportata.

FIGURA 3-3. Schermata Parole chiave

4. Selezionare una o più parole chiave e fare clic sulla freccia a destra (>). Le parole chiave selezionate appaiono nell'elenco "Selezionato", nella parte destra della schermata.
5. Opzionalmente, fare clic su **Aggiungi** per creare una nuova parola chiave, su **Modifica** per modificarne una esistente, su **Copia** per creare una copia (per la modifica) oppure su **Elimina**.
6. Fare clic su **Fine**. Hosted Email Security registra le selezioni e viene nuovamente visualizzata la schermata principale del passaggio 2: Seleziona parametri di scansione.
7. Ripetere i passaggi sopra riportati per ciascuna parte dell'e-mail a cui applicare il filtro del contenuto.
8. Una volta completata l'aggiunta di criteri di filtraggio avanzati, selezionare **Tutte le corrispondenze** (valore predefinito) oppure **Qualsiasi corrispondenza** nella colonna a destra di "Avanzati" per configurare la corrispondenza dell'e-mail a tutti i criteri selezionati o a uno qualsiasi dei criteri, per l'attivazione della regola.
9. Fare clic su **Avanti** e completare la regola come spiegato in *Aggiunta di una nuova regola* a pagina 3-27.

Filtraggio dei contenuti con le espressioni regolari

Per configurare il filtro dei contenuti utilizzando le espressioni regolari, effettuare quanto segue:

1. Seguire da *Passaggio 1* a *Passaggio 3* per visualizzare la schermata Parole chiave.
2. Fare clic su **Aggiungi** per creare una nuova parola chiave oppure selezionarne una esistente e fare clic su **Modifica.** Viene visualizzata nuovamente la schermata Parole chiave con un diverso layout, come mostrato nella *figura 3-4* sotto riportata.

FIGURA 3-4. Schermata Parole chiave per le espressioni regolari

3. Nel campo **Nome elenco**, immettere un nome per l'espressione, nel caso se ne stia creando una nuova. Se si modifica un'espressione, questo campo verrà popolato con il nome esistente.
4. Nell'elenco a discesa **Corrispondenza**, selezionare una delle seguenti opzioni:
   - **Qualsiasi specificata:** la corrispondenza si verifica quando nel contenuto si trova una qualsiasi delle parole chiave o delle espressioni regolari elencate.
   - **Tutte quelle specificate:** la corrispondenza si verifica quando nel contenuto si trovano tutte le parole chiave e/o espressioni regolari elencate.
   - **Non quelle specificate:** equivalente all'operatore.NOT., la corrispondenza si verifica se nel contenuto non si trova alcuna delle parole chiave o espressioni regolari elencate.

- **Solo quando il punteggio combinato supera la soglia:** quando selezionata, questa opzione visualizza al di sotto di essa il campo "Punteggio totale del messaggio per attivare l'azione". Quando è selezionata questa opzione, Hosted Email Security filtra il contenuto per le espressioni nell'elenco, se il punteggio totale dei messaggi e-mail di spam supera il valore di soglia immesso (il valore predefinito è 2).

5. Fare clic su **Aggiungi**. Viene visualizzata la schermata Aggiungi parole chiave.
6. Nella casella di testo, digitare una qualsiasi combinazione di parole chiave ed espressioni regolari per definire una parola chiave (senza interruzioni riga). Gli operatori di espressioni regolari disponibili sono mostrati di seguito:

   \ | ( ) { } [ ] . ^ $ * + ?

Suggerimento: Per utilizzare un operatore di espressione regolare come un carattere letterale, è necessario posizionare una carattere di barra rovesciata (\) immediatamente prima di esso. Trend Micro consiglia di utilizzare le espressioni regolari solo se si ha dimestichezza nell'utilizzo. Hosted Email Security non accetta espressioni immesse con sintassi regex non corretta.

---

7. Fare clic su **Salva.** Nella schermata Parole chiave viene visualizzata una tabella che elenca le parole chiave create, come mostrato nella *figura 3-5* sotto riportata.

FIGURA 3-5. Le parole chiave sono state appena aggiunte

8. Selezionare la casella di controllo **Maiuscole/minuscole** come appropriato. Se è stato selezionato **Solo quando il punteggio combinato supera la soglia** per il campo Corrispondenza e sono state aggiunte più parole chiave, selezionare il punteggio ponderato per ciascuna espressione, come spiegato in *Assegnazione di un peso agli elenchi di parole chiave* a pagina 3-11.
9. Fare clic su **Salva**. L'elenco di parole chiave appena create appare nell'elenco "Disponibile" nella casella a sinistra, come mostrato nella *figura 3-6* sotto riportata.

FIGURA 3-6. Aggiunta di una parola chiave a una regola

10. Per aggiungere il nuovo criterio alla regola, selezionare il nome dell'elenco nella casella a sinistra, fare clic sulla freccia a destra (>), quindi fare clic su **Fine**. Hosted Email Security aggiunge il criterio alla regola che si sta creando.
11. Fare clic su **Avanti** e completare la regola come spiegato in *Aggiunta di una nuova regola* a pagina 3-27.

Assegnazione di un peso agli elenchi di parole chiave

Quando si crea un elenco di parole chiave, è possibile assegnare un fattore ponderale a ciascuna parola chiave nell'elenco.

Quando l'opzione Corrispondenza è impostata su "Solo quando il punteggio combinato supera la soglia", è necessario impostare sia un punteggio complessivo per la parola chiave che un punteggio individuale per ciascun componente.

Per utilizzare l'assegnazione di un peso agli elenchi di parole chiave:

1. Assicurarsi di aver selezionato **Solo quando il punteggio combinato supera la soglia** nell'elenco a discesa Corrispondenza.
2. Digitare un peso totale nel campo **Punteggio totale del messaggio per attivare l'azione**.
3. Selezionare un peso per ciascuna espressione nell'elenco, dagli elenchi a discesa nella colonna **Punteggio**, come mostrato nella *figura 3-7* sotto riportata.

FIGURA 3-7. Assegnazione di un peso alle parole chiave

4. Opzionalmente, selezionare la casella di controllo **Maiuscole/minuscole** per ciascun elenco di parole chiave.
5. Fare clic su **Salva**.

Per ciascuna parola chiave elencata corrispondente al contenuto di un messaggio e-mail, Hosted Email Security incrementa il punteggio del messaggio nella colonna Punteggio relativa a quell'elenco. Ad esempio, se due parole contenute in un messaggio corrispondono alle parole di un elenco di parole chiave denominato "Volgarità", con il punteggio di 2, il punteggio del messaggio sarà 4.

Se il punteggio totale supera il numero riportato nel campo "Punteggio totale del messaggio per attivare l'azione", la regola viene attivata. Ad esempio, se vengono attivate due corrispondenze dell'elenco parole chiave per un punteggio del messaggio pari a 4, il valore del campo Punteggio totale del messaggio per attivare l'azione è 3 e la regola viene attivata.

Azioni per le regole

Hosted Email Security fornisce una serie di azioni utilizzabili per creare o modificare una regola. Le azioni disponibili per gli utenti di Hosted Email Security sono le seguenti:

- *Elimina intero messaggio* a pagina 3-13
- *Consegna il messaggio adesso* a pagina 3-14
- *Metti in quarantena il messaggio* a pagina 3-15
- *Disinfetta i file disinfettabili ed elimina i file non disinfettabili* a pagina 3-15
- *Elimina gli allegati corrispondenti* a pagina 3-16
- *Inserimento di un'azione Timbra nel corpo del messaggio* a pagina 3-17
- *Contrassegna la riga dell'oggetto* a pagina 3-17
- *Invia un messaggio di notifica* a pagina 3-18
- *Metti in Ccn un altro destinatario* a pagina 3-19
- *Rifiutare il messaggio* a pagina 3-19
- *Ignorare una regola* a pagina 3-20
- *Crittografa messaggio e-mail* a pagina 3-20 (venduto separatamente)

Queste azioni vengono eseguite in un ordine predefinito in base alla logica di elaborazione integrata in Hosted Email Security. Per ulteriori informazioni sull'ordine di esecuzione, vedere *Esecuzione dell'ordine di regole* a pagina 3-25.

Elimina intero messaggio

Questa azione elimina il messaggio e tutti gli allegati. Nei registri di Hosted Email Security il messaggio viene registrato come eliminato; dopo l'eliminazione, non è più possibile recuperare il messaggio. L'azione ricade nella categoria Intercetta (vedere *Azioni Intercetta* a pagina 3-25).

Per configurare un'azione per una regola con cui eliminare un messaggio:

1. Selezionare l'azione **Elimina intero messaggio** nella sezione Intercetta.
2. Se si sta creando una nuova regola, fare clic su **Avanti**; se invece si sta modificando una regola esistente, fare clic su **Salva**.

Consegna il messaggio adesso

Utilizzare l'azione Recapita subito per consegnare immediatamente i messaggi e-mail. Quando l'azione viene eseguita, Hosted Email Security consegna il messaggio e-mail senza applicare ulteriori regole al messaggio in questione.

Tutte le regole vengono ordinate automaticamente per migliorare l'efficienza a livello di sicurezza ed esecuzione. Gli amministratori non devono più determinare l'ordine di esecuzione delle regole. L'azione Recapita subito consente di bypassare l'ordinamento automatico dell'esecuzione per far sì che Hosted Email Security consegni il messaggio immediatamente.

ATTENZIONE! **Si sconsiglia l'uso di "Recapita subito" come unica azione. Se si sceglie "Recapita subito" come unica azione per la posta di spam, ad esempio, tutta la posta viene consegnata ai rispettivi destinatari come se non fosse stato attivato alcun filtro anti-spam.**

Se si utilizza "Recapita subito" con una regola antivirus, assicurarsi di avere attivato l'azione "Elimina" per la regola virus. L'azione "Elimina" è l'unica ad avere la precedenza su "Recapita subito" e viene quindi elaborata prima di essa, concludendo quindi l'elaborazione della regola.

Per configurare l'azione di una regola affinché un messaggio venga consegnato immediatamente:

1. Selezionare l'azione **Recapita subito** dalla sezione Intercetta.
2. Se si sta creando una nuova regola, fare clic su **Avanti**; se invece si sta modificando una regola esistente, fare clic su **Salva**.
3. Fare clic su **OK** nel messaggio di avviso Recapita subito che viene visualizzato. Il messaggio si chiude.
4. Se si crea una nuova regola, immettere un nome per la regola nel campo **Nome regola**.
5. Fare clic su **Salva**.

ATTENZIONE! **Se si sceglie "Recapita subito" come unica azione per la regola virus, è possibile che i messaggi e-mail che contengono virus riescano a filtrare senza essere bloccati.**

Metti in quarantena il messaggio

Se il livello di servizio comprende l’azione "Metti in quarantena", questa azione inserisce il messaggio e tutti gli allegati nell’area di quarantena configurata nella regola. L’azione ricade nella categoria Intercetta (vedere *Azioni Intercetta* a pagina 3-25).

Per configurare un’azione per una regola con cui mettere un messaggio in quarantena:

1. Nella sezione Intercetta della finestra Azione regola, selezionare l’azione **Metti in quarantena**.
2. Selezionare un’area di quarantena dall’elenco a discesa, oppure fare clic su **Modifica** per creare una nuova area di quarantena.

Nota: Gli elementi messi in quarantena vengono ora memorizzati in una struttura di directory creata da Hosted Email Security. Ciò consente di ottenere prestazioni migliori quando il prodotto sta salvando degli elementi nelle directory di quarantena o quando gli utenti visualizzano tali elementi mediante la console Web. I messaggi inseriti in quarantena vengono indicizzati nel database di Hosted Email Security per l’utilizzo di funzioni di interrogazione e strumenti di ricerca avanzata.

---

3. Se si sta creando una nuova regola, fare clic su **Avanti**; se invece si sta modificando una regola esistente, fare clic su **Salva**.

Disinfetta i file disinfettabili ed elimina i file non disinfettabili

Questa azione permette di disinfettare i file dai virus (o da altre minacce configurate) eliminabili contenuti negli allegati dei messaggi. Se non è possibile disinfettare il file dalla minaccia, l’allegato che la contiene viene eliminato. Disinfetta i file disinfettabili ricade nella categoria Intercetta (vedere *Azioni Modifica* a pagina 3-26).

Nota: L'azione "Disinfetta i file disinfettabili" è disponibile soltanto se il parametro antivirus nella definizione della regola è selezionato. Ad esempio:

Se nella regola viene usata questa azione e un messaggio contiene un virus non disinfettabile, il messaggio viene eliminato.

Se nella stessa regola vengono utilizzate le azioni "Elimina gli allegati corrispondenti" e "Disinfetta i file disinfettabili", un allegato che viola le regole viene eliminato immediatamente e l'azione "Disinfetta i file disinfettabili" non viene eseguita.

Per configurare un'azione per una regola con cui disinfettare gli allegati contenenti virus:

1. Nella sezione Modifica della schermata Azione, selezionare l'azione **Disinfetta i file infetti da virus**.
2. Se si sta creando una nuova regola, fare clic su **Avanti**; se invece si sta modificando una regola esistente, fare clic su **Salva**.

Elimina gli allegati corrispondenti

Questa azione elimina tutti gli allegati che corrispondono ai parametri della regola. L'azione ricade nella categoria Modifica (vedere *Azioni Modifica* a pagina 3-26).

Nota: L'azione Elimina gli allegati corrispondenti viene attivata soltanto se in una regola vengono utilizzati i parametri Dimensione, Allegato, Contenuto e/o Virus. Ad esempio, una regola anti-spam che prevedere un'azione "Elimina allegati corrispondenti" non ha effetto sul messaggio.

Per configurare un'azione per una regola con cui eliminare gli allegati che soddisfano un parametro, procedere come segue:

1. selezionare **Elimina gli allegati corrispondenti** nella sezione Modifica.
2. Se si sta creando una nuova regola, fare clic su **Avanti**; se invece si sta modificando una regola esistente, fare clic su **Salva**.

Inserimento di un'azione Timbra nel corpo del messaggio

L'azione "Inserisci timbro" inserisce un blocco di testo nel corpo del messaggio. I timbri sono gestiti come oggetti con nome all'interno del database e sono selezionabili da un elenco. Le definizioni dei timbri contengono il testo del timbro (che può contenere variabili di Hosted Email Security), l'impostazione di inserimento del timbro all'inizio o alla fine del corpo del messaggio e l'impostazione di attivazione o disattivazione dell'aggiunta del timbro nei messaggi TNEF (Transport Neutral Encapsulation Format) e con firma digitale allo scopo di evitarne il danneggiamento.

Per configurare un'azione per una regola con cui inserire un timbro nel corpo del messaggio:

1. Selezionare la casella di controllo **Inserisci timbro nel corpo**.
2. Fare clic su **Modifica**. Viene visualizzata la schermata Timbri che mostra un elenco a discesa di timbri disponibili.
3. Selezionare un timbro dall'elenco oppure fare clic su **Aggiungi**, **Modifica** o **Copia** per creare un nuovo timbro o modificarne uno esistente.
4. Fare clic su **Fine**.

Contrassegna la riga dell'oggetto

L'azione "Contrassegna oggetto" inserisce del testo configurabile nella riga dell'oggetto del messaggio. L'azione ricade nella categoria Modifica (vedere *Azioni Modifica* a pagina 3-26).

Per configurare un'azione per una regola con cui contrassegnare l'oggetto del messaggio:

1. Selezionare la casella di controllo **Contrassegna oggetto**.
2. Fare clic sul collegamento contrassegno per aprire la schermata di modifica dei contrassegni.
3. Digitare un contrassegno nel campo Contrassegno.
4. Selezionare o deselezionare la casella di controllo **Non contrassegnare i messaggi firmati digitalmente**.
5. Fare clic su **Salva**.

Invia un messaggio di notifica

Le notifiche sono messaggi che vengono inviati all'attivazione della regola. L'azione ricade nella categoria Monitora (vedere *Azioni Monitora* a pagina 3-26).

Per configurare un messaggio di notifica:

1. Nella sezione Monitora della schermata Azione, selezionare la casella di controllo **Invia una notifica** e fare clic sul collegamento **messaggio alla persona**.
2. Selezionare una notifica esistente e fare clic su **Modifica**, oppure fare clic su **Aggiungi** per creare un nuovo messaggio di notifica. Viene visualizzata la schermata Aggiungi regola > Notifiche.
3. Assegnare un nome alla notifica.
4. Digitare un indirizzo nel campo **Da**. Questo indirizzo appare nel campo del mittente quando il messaggio di notifica viene visualizzato dai destinatari e può essere utilizzato per nascondere Hosted Email Security agli utenti interni o ai destinatari esterni del messaggi.
5. Digitare un indirizzo nel campo **A**. Questo indirizzo viene utilizzato quando il messaggio di notifica viene inviato all'amministratore.
6. Selezionare i destinatari della notifica:
   - Fare clic su **Mittente** per inviare il messaggio di notifica al mittente.
   - Fare clic su **Destinatario** per inviare il messaggio di notifica al destinatario (disponibile unicamente se previsto dal livello di servizio).
   - Selezionare **Trap SNMP** per inviare la notifica mediante SNMP. Se si seleziona SNMP, selezionare anche il primo dei due pulsanti di opzione e scegliere il codice categoria appropriato (disponibile unicamente se previsto dal livello di servizio).
7. Digitare l'oggetto del messaggio. Se necessario, utilizzare le variabili.
8. Selezionare **Allega** per allegare una copia del messaggio originale al messaggio di notifica, quindi selezionare **Messaggio modificato** o **Messaggio non modificato** dal menu a discesa.

ATTENZIONE! **Se si seleziona "Messaggio non modificato" si può causare l'ingresso di messaggi o allegati infetti nell'ambiente di messaggistica. Trend Micro sconsiglia vivamente di scegliere questa impostazione, a meno che non sia assolutamente necessario analizzare i messaggi nella loro forma non modificata.**

---

9. Digitare il corpo del messaggio di notifica nel campo **Testo**. Fare clic sul collegamento **Elenco variabili** per visualizzare le variabili disponibili nei messaggi di notifica.
10. Fare clic su **Salva**.

Metti in Ccn un altro destinatario

L'azione Ccn invia una Ccn (copia nascosta) al destinatario o ai destinatari configurati nella regola. L'azione ricade nella categoria Monitora (vedere *Azioni Monitora* a pagina 3-26).

È possibile configurare l'invio di una notifica soltanto a un indirizzo compreso nel proprio dominio.

Per configurare un'azione relativa a una regola con cui inviare la copia di un messaggio a un destinatario Ccn:

1. Nella sezione Monitora della schermata Azione, selezionare la casella di controllo Ccn.
2. Digitare nel campo l'indirizzo e-mail del destinatario. Per effettuare l'invio a più indirizzi e-mail, digitare gli indirizzi nel campo separandoli con delle virgole.
3. Se si sta creando una nuova regola, fare clic su **Avanti.** Se si sta modificando una regola esistente, fare clic su **Salva**.

Rifiutare il messaggio

L'azione Rifiuta blocca il messaggio contenente determinati tipi di allegati per l'MTA upstream. Il messaggio viene registrato come rifiutato nei registri Hosted Email Security. Tuttavia, una volta rifiutato, non è possibile recuperare il messaggio.

Nota: L'azione di rifiutare il messaggio è disponibile solo per criteri che proteggono da virus o malware.

Per configurare un'azione regola Limiti di scansione per rifiutare un messaggio:

1. Selezionare l'azione **Rifiuta il messaggio** dalla sezione Limiti di scansione.
2. Fare clic su **Avanti** nel caso in cui si stia creando una nuova regola o su **Salva**, se si sta modificando una regola esistente.

Ignorare una regola

L'azione Ignora, consente di ignorare la regola specificata e di continuare a verificare il messaggio rispetto alle rimanenti regole del criterio. L'azione viene registrata come ignorata nei registri Hosted Email Security.

Nota: L'azione di ignorare questa regola è disponibile solo per criteri che proteggono da virus o malware.

Per configurare un'azione regola Limiti di scansione per ignorare un messaggio:

1. Selezionare l'azione **Ignora questa regola** dalla sezione Limiti di scansione.

   ATTENZIONE! Il messaggio consegnato potrebbe contenere un rischio per la protezione.

   ---

2. Fare clic su **Avanti** nel caso in cui si stia creando una nuova regola o su **Salva**, se si sta modificando una regola esistente.

Crittografa messaggio e-mail

Scopo di questa regola è proteggere i dati sensibili contenuti nei messaggi e-mail e inviati da utenti all'interno della rete aziendale. Il servizio Crittografia e-mail utilizza l'architettura Hosted Email Security esistente. Quando un messaggio e-mail attiva una regola di filtraggio del contenuto che contiene un'azione di crittografia, Hosted Email Security invia il messaggio e-mail al server di crittografia Hosted Email Security, che crittografa il messaggio e lo inoltra all'MTA in uscita.

Si tratta di un'azione univoca: è un'azione non finale che non può coesistere con nessun'altra azione (finale o non finale) all'interno della medesima regola. e si applica esclusivamente alle regole di posta in uscita.

Nella maggior parte dei casi, una regola per la crittografia di un messaggio e-mail sia basa su:

- Mittenti o destinatari del messaggio specifici (ad esempio, una regola che crittografa tutti i messaggi e-mail inviati dal reparto Risorse umane o Legale)
- Contenuto specifico del corpo del messaggio

Per le direttive dettagliate sull'impostazione delle parole chiave con il filtro dei contenuti, consultare *Filtro dei contenuti* a partire da pagina 3-6.

Per configurare una nuova regola di crittografia dei messaggi e-mail:

1. Nel menu di sinistra, fare clic su **Criterio**. Viene visualizzata la schermata Criterio.
2. Fare clic su **Aggiungi**. Viene visualizzata la schermata Aggiungi regola / Fase 1: Seleziona destinatari e mittenti.
3. Selezionare **Messaggio in uscita** dall'elenco a discesa "Questa regola si applica a".
4. Fare clic sul collegamento **Mittenti** e selezionare uno o più indirizzi o domini.
5. Fare clic su **Salva** per chiudere la schermata, quindi fare clic su **Avanti** per passare alla schermata del passaggio 2: Schermata Seleziona parametri di scansione.
6. Accettare il valore predefinito "Nessun parametro" oppure fare clic su **Avanzato**. Al di sotto di questa opzione vengono visualizzate alcune opzioni.
7. Dall'elenco, selezionare l'opzione che esegue la scansione del messaggio in base a un particolare contenuto, ad esempio, **L'oggetto corrisponde a, Il corpo corrisponde a, L'intestazione specificata corrisponde a** oppure **Il contenuto dell'allegato corrisponde a.**
8. Fare clic sul collegamento della parola chiave accanto all'opzione selezionata e aggiungere una o più parole chiave come spiegato in *Filtro dei contenuti* a partire da pagina 3-6.
9. Fare clic su **Avanti.** Viene visualizzata la schermata Aggiungi regola / Fase 3: Seleziona azioni.
10. Accettare la scelta predefinita "Non intercettare i messaggi" e andare alla sezione "Modifica".
11. Selezionare la casella di controllo **Crittografa e-mail** e fare clic su **Avanti**. Viene visualizzata la schermata Aggiungi regola / Fase 4: Nome e note.
12. Immettere un nome per la nuova regola e fare clic su **Salva.** Hosted Email Security ritorna alla schermata Criterio con la nuova regola evidenziata in giallo.

Lettura di messaggi e-mail crittografati

Quando viene attivata una regola "Crittografa e-mail", un destinatario ha la possibilità di decrittografare un messaggio crittografato in due modi. Il primo modo consiste nell'acquisto di Trend Micro Email Encryption Client. Per ulteriori informazioni su questo prodotto, consultare la seguente pagina sul sito Web di Trend Micro:

http://it.trendmicro.com/it/products/enterprise/email-encryption/

Se non si utilizza questo client, il destinatario riceve una notifica simile a quella mostrata nella *figura 3-8* a pagina 3-22.

Nota: Non è possibile decrittografare il messaggio crittografato con Microsoft Outlook Web Access 2007.

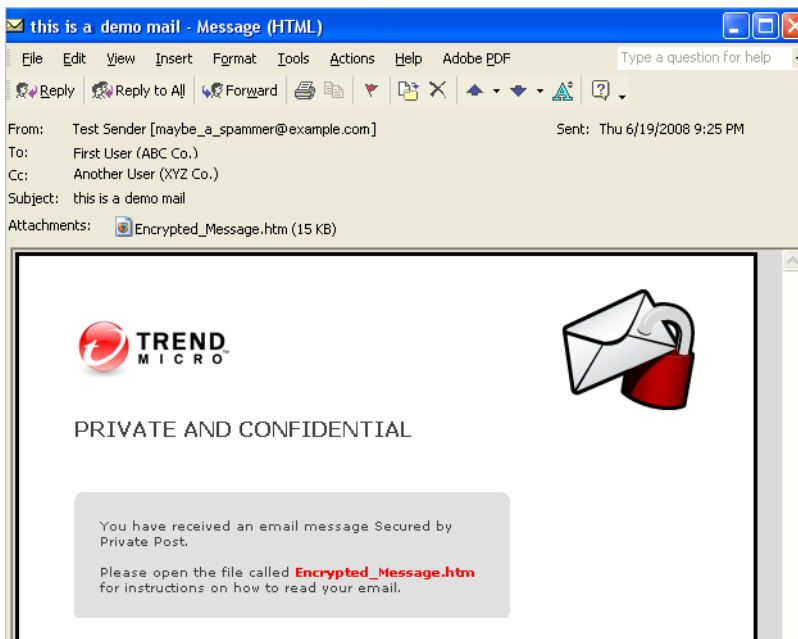



FIGURA 3-8. Notifica di un messaggio crittografato

Per recuperare un'e-mail crittografata, il destinatario deve effettuare quanto segue:

1. Fare doppio clic sul file "Encrypted_Message.htm", che si aprirà nel browser predefinito dell'utente, come mostrato nella *figura 3-9*.

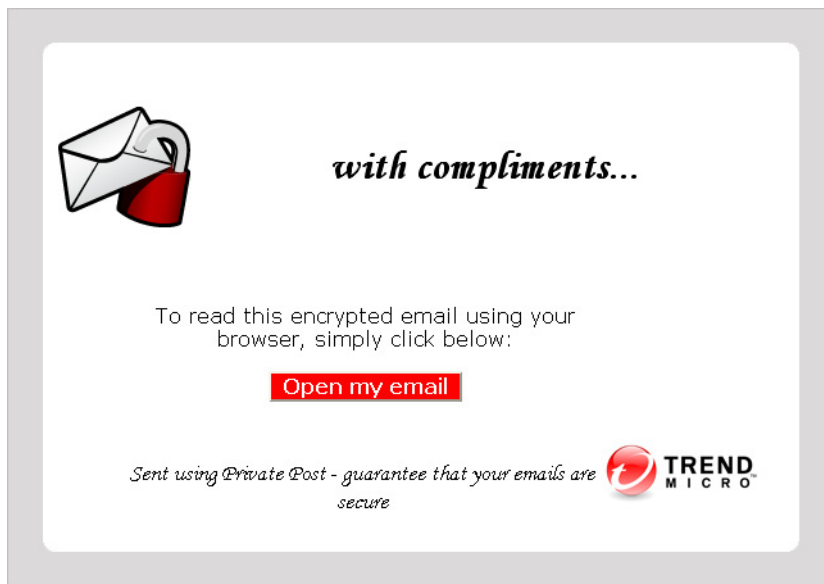



FIGURA 3-9. Encrypted_Message.htm come visualizzato nel browser

2. Fare clic sull'opzione per l'**apertura dell'e-mail** e se non è stata ancora effettuata la registrazione, immettere le informazioni sulla registrazione nelle pagine successive. Se è stata già effettuata la registrazione per questo servizio, sul sito di crittografia viene visualizzata l'e-mail decrittografata.

Nota: La funzione per l'apertura dell'e-mail potrebbe non essere eseguita correttamente con alcuni sistemi di posta basati su Web. Se il pulsante non funziona, l'utente può salvare l'allegato su un computer locale e poi aprirlo.

3. Per una sicurezza avanzata, utilizzare un'immagine di verifica CAPTCHA, immettere e confermare la frase segreta, quindi selezionare e rispondere alle tre domande di sicurezza. Una volta eseguita la registrazione, il sito di crittografia e-mail invia un messaggio di attivazione all'account e-mail del destinatario.

4. Una volta ricevuto il messaggio di attivazione, fare clic sull'opzione indicante di **fare clic in questo punto per convalidare l'identità.** Il sito di crittografia e-mail di Trend Micro viene caricato nel browser e visualizza il messaggio decrittografato, come mostrato nella *figura 3-10* a pagina 3-24.

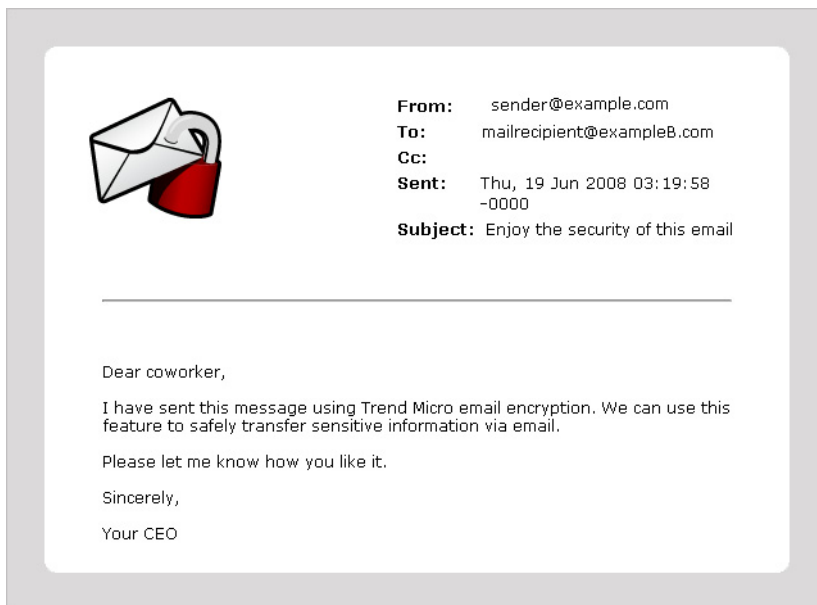



FIGURA 3-10. Decrittografia messaggio e-mail

Nota: Occorre registrare i destinatari una sola volta. Dopo aver effettuato la registrazione con il servizio di crittografia e-mail, il destinatario potrà visualizzare l'e-mail decrittografata in una finestra del browser facendo clic sull'opzione per l'**apertura dell'e-mail**.

Esecuzione dell'ordine di regole

Tutte le regole vengono ordinate automaticamente per migliorare l'efficienza a livello di sicurezza ed esecuzione. Gli amministratori non devono più determinare l'ordine di esecuzione delle regole. Esistono quattro tipi di azioni in una regola:

- *Azioni Intercetta*
- *Azioni Modifica*
- *Azioni Monitora*
- *Limiti di scansione*
- *Azione Crittografia e-mail*

Azioni Intercetta

Quando viene eseguita un'azione Intercetta o "terminale", l'elaborazione della regola si interrompe e per essa non viene più eseguita alcuna azione.

Le azioni Intercetta vengono eseguite secondo un rigido ordine di priorità:

1. Elimina tutto il messaggio
2. Consegna il messaggio adesso (consultare la nota a pagina 3-31)
3. Metti in quarantena il messaggio
4. Reindirizza a un altro destinatario e-mail

Nota importante sull'azione Recapita subito

Si sconsiglia l'uso di "Recapita subito" come unica azione. Se si sceglie "Recapita subito" come unica azione per la posta di spam, ad esempio, tutta la posta viene consegnata ai rispettivi destinatari come se non fosse stato attivato alcun filtro anti-spam.

Se si utilizza "Recapita subito" con una regola antivirus, assicurarsi di avere attivato l'azione "Elimina" per la regola virus. L'azione "Elimina" è l'unica ad avere la precedenza su "Recapita subito" e viene quindi elaborata prima di essa, concludendo quindi l'elaborazione della regola.

ATTENZIONE! **Se si sceglie "Recapita subito" come unica azione per la regola virus, è possibile che i messaggi e-mail che contengono virus riescano a filtrare senza essere bloccati.**

Azioni Modifica

Le seguenti azioni "modifica" (non finali) eseguono ma non terminano l'elaborazione (i messaggi e-mail vengono consegnati ai destinatari originali):

- Disinfetta virus disinfettabili
- Elimina allegato
- Inserisci un timbro nel corpo del messaggio
- Contrassegna la riga dell'oggetto

Suggerimento: Le azioni finali hanno una maggiore priorità di esecuzione rispetto a quelle non finali. Quando viene attivata un'azione finale, non è necessario eseguire altre azioni. Tuttavia, è possibile combinare azioni non finali come "Elimina un allegato" e "Timbra il corpo del messaggio".

Azioni Monitora

Sono presenti due azioni relative al monitoraggio.

- Invia un messaggio di notifica
- Metti in Ccn un altro destinatario

È possibile combinare la prima azione con qualsiasi altra azione, ad esempio, l'azione Ccn con le azioni per la "modifica" (e con la prima azione per il "monitoraggio"). In ogni caso, non è possibile combinare l'azione Ccn con le azioni finali (di intercettazione).

Suggerimento: Il messaggio e-mail di notifica inviato per monitorare le azioni può essere personalizzato utilizzando le variabili mostrate nella Guida in linea.

Limiti di scansione

Sono presenti due trigger per il limite di scansione:

- Il file 2007 contiene più di 353 file.
- L'archivio compresso contiene più di 353 file.
- Il file Office 2007/2010 contiene un file con una percentuale di decompressione maggiore di 100.
- Il file compresso contiene un file con una percentuale di decompressione maggiore di 100.

I limiti di scansione possono essere utilizzati solo con criteri che proteggono da virus/malware. Possono essere combinati con azioni di modifica o finali.

Azione Crittografia e-mail

Questa funzione è disponibile solo per gli utenti di Hosted Email Security.

L'azione Crittografa messaggio e-mail di Trend Micro è disponibile solo se questa opzione viene acquistata separatamente. Il servizio di crittografia e-mail è disponibile solo per gli utenti di Hosted Email Security che hanno abilitato il filtraggio della posta in uscita. Si tratta di un'azione univoca: è un'azione non finale che non può coesistere con nessun'altra azione (finale o non finale) all'interno della medesima regola. Se a un messaggio si applica più di una regola, Hosted Email Security elabora la regola che utilizza l'azione di crittografia e-mail dopo aver elaborato tutte le altre regole.

Nota: Tenere presente che "non intercettare" non è considerata un'azione.

Aggiunta e modifica di regole

Solo gli utenti Hosted Email Security possono aggiungere, modificare, copiare o eliminare le regole. Per istruzioni dettagliate, vedere le sezioni seguenti.

Aggiunta di una nuova regola

Le regole sono i mezzi attraverso i quali i criteri dei messaggi vengono applicati al traffico in Hosted Email Security. Ogni regola è costituita da tre parti principali:

- L'utente o il dominio a cui si applica la regola.
- I parametri valutati per determinare se la regola deve essere attivata.
- L'azione eseguita da Hosted Email Security se la regola viene attivata.

Dopo che queste tre parti della regola sono state configurate, alla regola viene assegnato un nome univoco con cui viene identificata nei riepiloghi, nella verifica posta e così via. Ogni regola può essere disabilitata senza perdere la definizione e quindi riabilitata in un secondo momento.

Per creare una nuova regola:

1. Fare clic su **Aggiungi** nella schermata Criterio. Viene visualizzata la schermata **Aggiungi regola**.

FIGURA 3-11. Schermata Aggiungi regola

2. Selezionare l'utente o il dominio a cui si applica la regola.

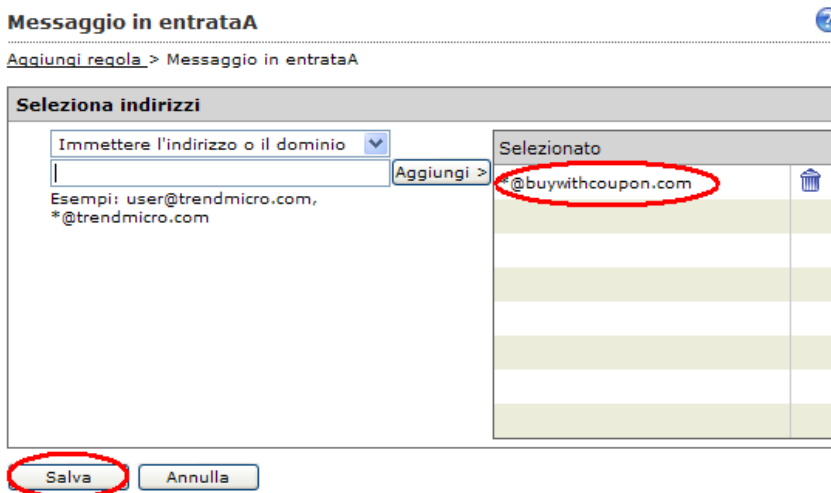



FIGURA 3-12. Aggiunta di un dominio o di utenti in questa schermata

3. Selezionare e configurare i parametri.

FIGURA 3-13. Selezionare i parametri per la regola nella schermata

4. Selezionare e configurare l'azione Intercetta.

FIGURA 3-14. Selezionare l'azione nella schermata

ATTENZIONE! **Si sconsiglia l'uso di "Recapita subito" come unica azione. Se selezionata, l'azione "Recapita subito" ha la precedenza su tutte le altre regole. Quindi, se occorre cercare dei criteri, non sarà possibile elaborarli.**

Se si sceglie "Recapita subito" come unica azione per la posta di spam, ad esempio, tutta la posta viene consegnata ai rispettivi destinatari come se non fosse stato attivato alcun filtro anti-spam.

Se si sceglie "Recapita subito" come unica azione per la regola virus, è possibile che i messaggi e-mail che contengono virus riescano a filtrare senza essere bloccati.

Se si tenta di impostare l'azione "Recapita subito", viene visualizzato il messaggio riportato *figura 3-15* di seguito.

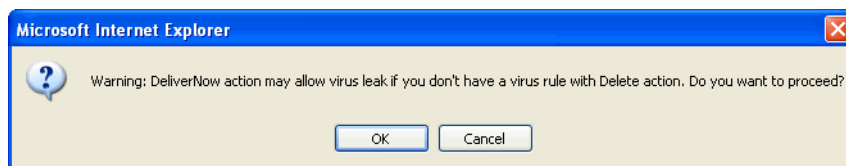
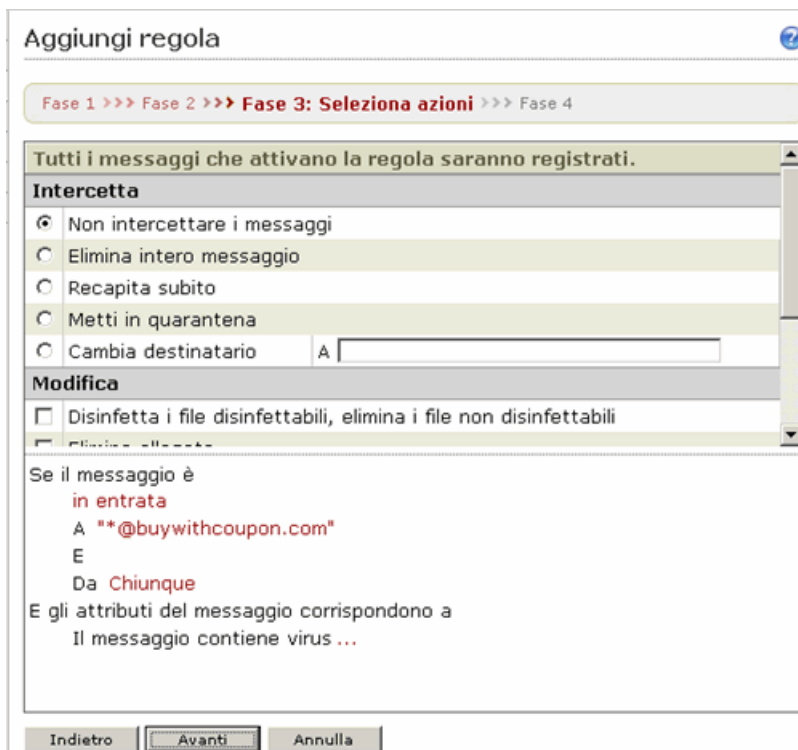



FIGURA 3-15. Messaggio di avviso Recapita subito

5. In alternativa, selezionare qualsiasi azione Modifica o Monitora, come indicato nella *figura 3-16* di seguito.

   Per criteri relative ai virus, è inoltre possibile selezionare le azioni Limiti di scansione.

FIGURA 3-16. Passaggio 3: selezione delle azioni Modifica e Monitora

6. Assegnare un nome alla regola e abilitarla.

FIGURA 3-17. Assegnare un nome e salvare la regola in questa schermata

7. Fare clic su **Salva**.

   Viene visualizzata la schermata **Criterio**, con la nuova regola nell'ordine appropriato ed evidenziata nell'elenco, come mostrato nella *figura 3-18* di seguito.

FIGURA 3-18. Schermata Criterio che mostra un criterio appena creato

Modifica di una regola esistente

Per modificare una regola esistente:

1. Nell'elenco delle regole, fare clic sul nome della regola da modificare.
2. Modificare la regola.

   L'esempio di seguito spiega come aggiungere un mittente approvato a questa regola.

   a. Fare clic sul collegamento **Se il messaggio è…** per modificare l'elenco delle eccezioni dei mittenti.

   b. Fare clic su **Eccezione** nella riga Mittente.

   c. Immettere l'indirizzo del mittente nella casella di testo per aggiungere un mittente approvato all'elenco delle eccezioni.

   Nell'esempio mostrato nella *figura 3-19* a pagina 3-35, "ceo@example.com" è stato escluso da questa regola.
3. Fare clic su **Salva** per salvare i mittenti approvati per questa regola. In questo modo vengono salvati i mittenti approvati, ma non la regola.

FIGURA 3-19. Modificare le eccezioni dei mittenti in questa schermata

4. Fare clic su **Salva** per continuare.

FIGURA 3-20. Schermata Modifica criterio

5. Fare nuovamente clic su **Salva** per salvare la regola.

FIGURA 3-21. Salvare le modifiche ai criteri in questa schermata.

Copia di una regola esistente

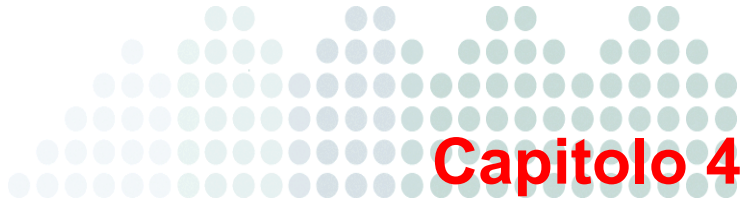
Spesso una nuova regola è molto simile a una regola già esistente. In questi casi, solitamente è più semplice copiare una regola e modificarla piuttosto che crearne una completamente nuova.

Per copiare una regola esistente:

1. Nell'elenco delle regole, selezionare la casella di controllo davanti alla regola da copiare.
2. Fare clic su **Copia**. Nell'elenco delle regole viene visualizzata una regola chiamata "Copia di [nome regola originale]".
3. Modificare la regola.

Eliminazione di una regola esistente

Per eliminare regole esistenti:

1. Nell'elenco delle regole, selezionare la casella di controllo davanti alla regola da eliminare.
2. Fare clic su **Elimina**.

Capitolo 4

Mittenti approvati, quarantena e registri

Questo capitolo fornisce informazioni utili per l'impostazione dei mittenti approvati, l'accesso alla quarantena, l'uso dei messaggi e-mail Digest di spam, l'uso di Web End User Quarantine e l'interpretazione dei registri di Hosted Email Security.

Gli argomenti trattati nel presente capitolo includono:

Mittenti approvati

La schermata Mittenti approvati consente agli amministratori dei sistemi di posta elettronica di approvare indirizzi e-mail o domini specifici, inserendoli nei domini gestiti.

Nota: La schermata è diversa dagli elenchi Approvati/Bloccati relativi alla reputazione IP (**Reputazione IP > Approvati/Bloccati**). In questa schermata è possibile impostare come attendibili determinati indirizzi e-mail o domini che non verranno sottoposti a scansione; la schermata Approvati/Bloccati in Reputazione IP fa invece riferimento esclusivamente alle verifiche della reputazione IP.

Per i mittenti approvati:

- Hosted Email Security non blocca eventuali messaggi e-mail provenienti dai mittenti (o domini) specificati.
- Le regole anti-spam euristiche basate sul contenuto non vengono applicate ai messaggi e-mail ricevuti dai mittenti o dai domini specificati.
- Tutte le regole relative a virus, contenuto e allegati vengono comunque applicate.

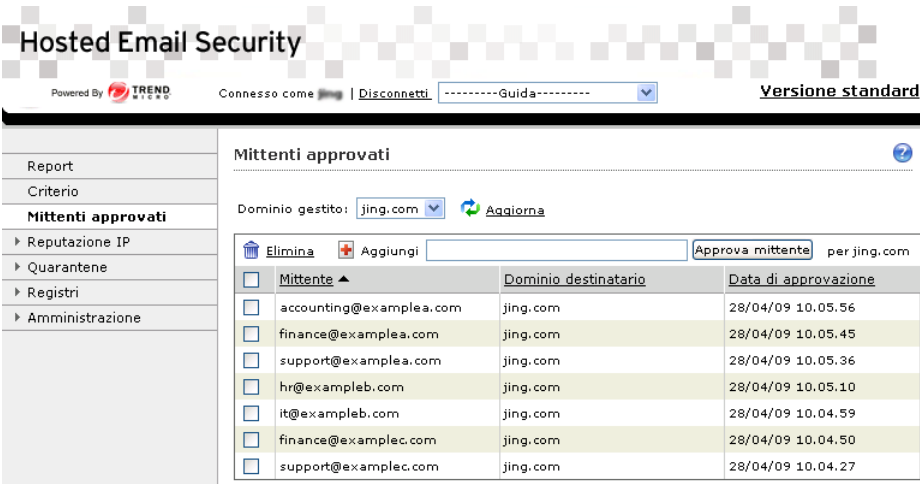



FIGURA 4-1. Schermata Mittenti approvati

Per aggiungere mittenti approvati:

1. Dall'elenco a discesa Dominio gestito, selezionare il dominio specifico (oppure "Tutti i domini") ai quali saranno aggiunti i mittenti approvati.
2. Fare clic su **Aggiorna**.
3. Immettere un singolo indirizzo o dominio nel campo **Aggiungi**.

   Esempio:

   - Per un singolo indirizzo, digitare: nome@esempio.com
   - Per un dominio, digitare: *@esempio.com
4. Fare clic su **Approva mittente**.

Per modificare una voce dell'elenco:

1. Fare clic sulla rispettiva voce.
2. Apportare le modifiche.
3. Fare clic su **OK**.

Per eliminare una voce:

1. Selezionare la casella di controllo relativa alla voce.
2. Fare clic su **Elimina**.

Metti in quarantena

Questa sezione si applica solo se il livello di servizio lo consente.

Query di quarantena

Questa schermata fornisce un elenco di tutti i messaggi in quarantena che soddisfano i parametri di query. Fornisce inoltre gli strumenti per la gestione di questi messaggi.

Per eliminare uno o più messaggi in quarantena:

1. Selezionare la casella di controllo davanti al messaggio o ai messaggi da eliminare.
2. Fare clic su **Elimina** per rimuovere in modo permanente i messaggi selezionati.

Per inviare nuovamente uno o più messaggi in quarantena:

1. Selezionare la casella di controllo davanti al messaggio o ai messaggi da inviare di nuovo.
2. Fare clic su **Recapita (non spam)** per togliere i messaggi selezionati dalla quarantena.

Nota: Se si fa clic su **Recapita (non spam)**, i messaggi selezionati verranno tolti dalla quarantena e saranno elaborati da Hosted Email Security (salvo che questa volta i parametri anti-spam non verranno applicati). Tuttavia, questi messaggi potrebbero non arrivare nella casella Posta in arrivo dei messaggi e-mail se violano altri criteri di sicurezza dei messaggi aziendali.

Per eliminare o inviare nuovamente tutti i messaggi dell'elenco:

1. Selezionare la casella di controllo accanto all'intestazione della colonna **Data** per selezionare tutti i messaggi. Hosted Email Security seleziona tutti i messaggi sulla schermata.
2. Fare clic su **Elimina** oppure su **Recapita (non spam)**. Hosted Email Security elimina tutti i messaggi nell'elenco.

Impostazioni quarantena

Nella schermata delle impostazioni di quarantena (Figura 4-2), è possibile configurare un messaggio e-mail Digest di riepilogo in cui siano elencati fino a 100 messaggi e-mail in quarantena. Questa messaggio fornisce un collegamento all'intestatario dell'account per accedere ai messaggi desiderati. Inoltre, è possibile abilitare l'intestatario dell'account all'approvazione dei messaggi in quarantena dall'interno del messaggio e-mail Digest, come spiegato di seguito.

Approvazione di messaggi o mittenti all'interno del messaggio e-mail Digest di spam (Azione Incorporata)

Dalla schermata Impostazioni di quarantena, è possibile abilitare un'azione incorporata dal messaggio e-mail Digest di spam, vale a dire, i destinatari dei messaggi e-mail Digest di spam possono approvare uno o più messaggi o mittenti direttamente dall'interno del messaggio stesso, utilizzando un modulo HTML.

Configurazione dell'Azione Incorporata digest di spam

Abilitando questa azione, è possibile avvertire gli utenti della necessità di effettuare l'accesso alla Quarantena utente finale e approvare manualmente i messaggi o i mittenti in quarantena.

Quarantine Settings

Managed Domain: *@example.com Enabled

Digest Mail Schedule for example.com

Daily Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Time: 12:00 AM UTC

Digest Mail Template for example.com

Sender's Email: %DIGEST_RCPT%

Subject: spam digest for %DIGEST_DATE%

(Maximum number of characters is 256.)

HTML content: Inline Action Disabled

```
<html><head><style>.data2b {BACKGROUND-COLOR: #ececdb;}
</style></head><body><br/><form id="02AE5E" method="post"
action="%EUQ_HOST_SERVER%/emailRequest.imhs"><table
border=1><tr
bgcolor="#d4d4d4"><td><b>Date:</b></td><td><b>From:</b></td
><td><b>Subject:</b></td></tr>%DIGEST_BODY_HTML%
</table></form> </br><b> %DIGEST_PAGE_COUNT%   of
  %DIGEST_TOTAL_COUNT%  
messsages</b></body></html>
```

Reset to Default HTML Content

Plain text content:

```
spam list
----------------------------------------------------------------------------
---------------------
Date:                From:                                  Subject:
----------------------------------------------------------------------------
---------------------
%DIGEST_BODY_TEXT%
----------------------------------------------------------------------------
---------------------
%DIGEST_PAGE_COUNT% of %DIGEST_TOTAL_COUNT% messages
```

Reset to Default Plain Text Content

Save Cancel

FIGURA 4-2. Impostazioni di quarantena per la configurazione del messaggio e-mail Digest

Per configurare il messaggio e-mail Digest di spam:

1. Dal menu a sinistra, fare clic su **Impostazioni > quarantena**. Viene visualizzata la schermata Impostazioni quarantena.
2. Sulla parte superiore destra della schermata, fare clic sull'icona **Disabilitato** per abilitare la funzione Digest di spam. È disabilitata per impostazione predefinita.
3. Selezionare il dominio gestito per cui verrà creato il messaggio e-mail Digest di spam.
4. Selezionare la frequenza con la quale inviare i messaggi Digest in quarantena:
   - Frequenza giornaliera.
   - In giorni specifici. Ad esempio, selezionare le caselle di controllo relative a lunedì, mercoledì e venerdì solo in quei giorni.

Nota: I messaggi e-mail in quarantena vengono conservati nella quarantena in Hosted Email Security accessibile via Web per 21 giorni nella regione EMEA e 15 giorni in tutti gli altri paesi.

---

5. Selezionare un'ora o un fuso orario per l'invio del messaggio e-mail Digest.
6. Impostare inoltre i seguenti elementi:
   - **E-mail mittente**: l'indirizzo e-mail che verrà visualizzato sulla riga "Da" del messaggio e-mail Digest.
   - **Oggetto**: il testo che viene visualizzato nella riga dell'oggetto del messaggio digest.
   - **Contenuto HTML**: il contenuto che verrà visualizzato se il client di posta dell'utente finale permette messaggi e-mail HTML (vedere la *figura 4-4*).
   - **Contenuto TESTO**: il contenuto che verrà visualizzato se il client di posta dell'utente finale permette solo messaggi e-mail di solo testo (vedere la *figura 4-3*).
7. Opzionalmente, fare clic con il pulsante destro su ciascun campo per visualizzare un menu a comparsa da cui selezionare i token disponibili. Vedere la descrizione dei token disponibili nella *tabella 4-1*.

Nota: Il dominio utilizzato nell'indirizzo e-mail del mittente deve corrispondere al dominio a cui il messaggio verrà consegnato.

TABELLA 4-1. Variabili per il modello dei messaggi e-mail Digest

CAMPO	TOKEN DISPONIBILI	QUANDO VIENE UTILIZZATO QUESTO TOKEN. . .
E-mail mittente	%DIGEST_RCPT%	L'indirizzo e-mail del destinatario Digest viene visualizzato nel campo Da: del messaggio Digest ricevuto.
Oggetto	%DIGEST_RCPT%	L'indirizzo e-mail del destinatario Digest viene visualizzato nella riga dell'oggetto.
	%DIGEST_DATE%	La data Digest viene visualizzata nella riga dell'oggetto.
Contenuto HTML	%DIGEST_RCPT%	L'indirizzo e-mail del destinatario Digest viene visualizzato nel corpo HTML del messaggio.
	%DIGEST_DATE%	La data Digest viene visualizzata nel corpo HTML del messaggio.
	%DIGEST_BODY_HTML%	Il riepilogo Digest in formato HTML viene visualizzato nel corpo HTML del messaggio.
	%DIGEST_TOTAL_COUNT%	Il numero totale di tutti i messaggi al momento in quarantena viene visualizzato nel corpo HTML del messaggio Digest.
	%DIGEST_PAGE_COUNT%	Il numero totale di messaggi in quarantena nel riepilogo Digest (massimo 100) viene visualizzato nel corpo HTML del messaggio Digest.

TABELLA 4-1. Variabili per il modello dei messaggi e-mail Digest (segue)

CAMPO	TOKEN DISPONIBILI	QUANDO VIENE UTILIZZATO QUESTO TOKEN. . .
Contenuto testo normale	%DIGEST_RCPT%	L'indirizzo e-mail del destinatario Digest viene visualizzato nel corpo testuale del messaggio.
	%DIGEST_DATE%	La data Digest viene visualizzata nel corpo del testo del messaggio.
	%DIGEST_BODY_TEXT%	Il riepilogo Digest in formato solo testo viene visualizzato nel corpo testuale del messaggio.
	%DIGEST_TOTAL_COUNT%	Il numero totale di tutti i messaggi al momento in quarantena viene visualizzato nel corpo solo testo del messaggio Digest.
	%DIGEST_PAGE_COUNT%	Il numero totale di messaggi in quarantena elencato nel riepilogo Digest (massimo 100) viene visualizzato nel corpo solo testo del messaggio Digest.

8. Opzionalmente, fare clic sull'icona "Disabilitato" (Disattivato) accanto ad "Azione Incorporata" al di sopra della casella di testo del contenuto HTML per abilitare l'azione incorporata, come descritto in *Approvazione di messaggi o mittenti all'interno del messaggio e-mail Digest di spam (Azione Incorporata)* a pagina 4-5. L'icona cambia in "Abilitato" (Enabled) e il digest spam inviato conterrà pulsanti di opzione e pulsanti di invio attraverso i quali l'utente può approvare i messaggi o i mittenti direttamente dall'interno del messaggio.
9. Fare clic su **Salva** per salvare le modifiche.

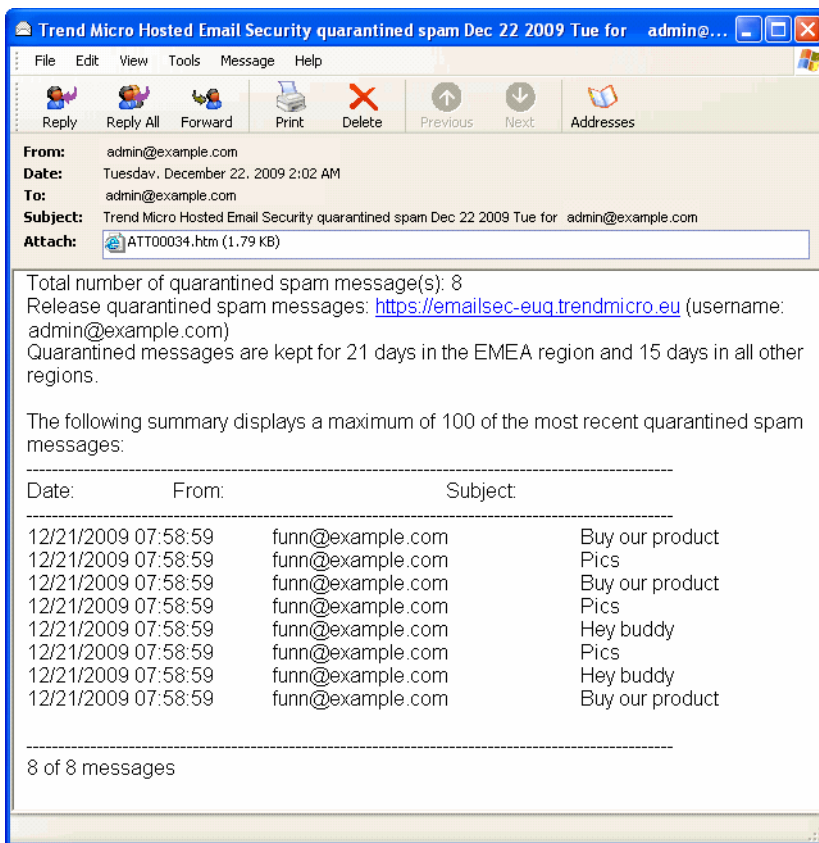



FIGURA 4-3. Messaggio e-mail Digest di testo di spam di esempio

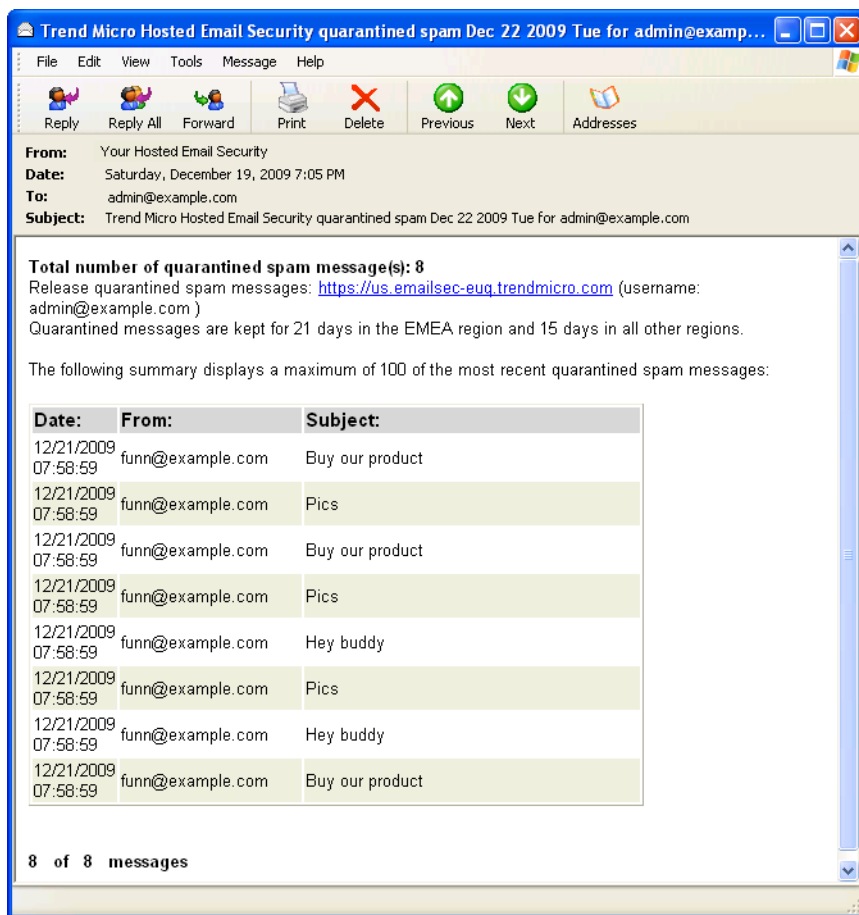



FIGURA 4-4. Messaggio e-mail Digest HTML di esempio con l’azione incorporata disabilitata (abbreviata per motivi di leggibilità)

Utilizzo dell'Azione Incorporata digest di spam

Poiché evita all'utente di dover accedere al sito Quarantena utente finale, l'azione incorporata digest di spam consente di risparmiare tempo. Quando si utilizza un client di posta con questa funzione, occorre tenere presente alcuni punti:

1. L'azione incorporata digest di spam supporta solo computer client che soddisfano i seguenti requisiti di sistema:
   - Microsoft Office XP, service pack 3
   - Microsoft Outlook 2003 (SP3) o Outlook Express 6.0
2. Facendo clic sulla riga dell'oggetto con collegamento ipertestuale di un messaggio, si apre una finestra del browser corrispondente alla schermata di accesso al sito EUQ.
3. Se si invia un messaggio con l'opzione "Non spam", il messaggio viene rimosso dalla quarantena. Se il messaggio viola più di un criterio di scansione, è possibile che, dopo la rielaborazione, il messaggio attivi un criterio diverso da quello che originariamente lo aveva posto in quarantena e che, pertanto, venga nuovamente posto in quarantena.
4. Se si invia un messaggio con l'opzione "Approva mittente (Non spam)", il messaggio viene rimosso dalla quarantena e il mittente del messaggio viene aggiunto all'elenco dei mittenti approvati.
5. Una volta inviato un messaggio per la rimozione dalla quarantena con l'opzione "Non spam", se successivamente si invia lo stesso messaggio ma con l'opzione "Mittente approvato (Non spam)", Hosted Email Security non aggiunge il mittente all'elenco dei mittenti approvati, in quanto il messaggio stesso non è più in quarantena; pertanto, Hosted Email Security non ha modo di identificare il mittente. Tuttavia sarà sempre possibile visualizzare il messaggio della schermata di risposta:
   ```
   Hosted Email Security ha ricevuto la richiesta di
   revisionare lo stato di spam di uno o più messaggi
   o mittenti.
   ```
6. Infine, è importante tenere presente quanto segue:

ATTENZIONE! **Chiunque riceva questo messaggio e-mail Digest di spam sarà in grado di aggiungere i mittenti al proprio elenco di mittenti approvati. Pertanto, Trend Micro raccomanda di non inoltrare il messaggio e-mail Digest di spam.**

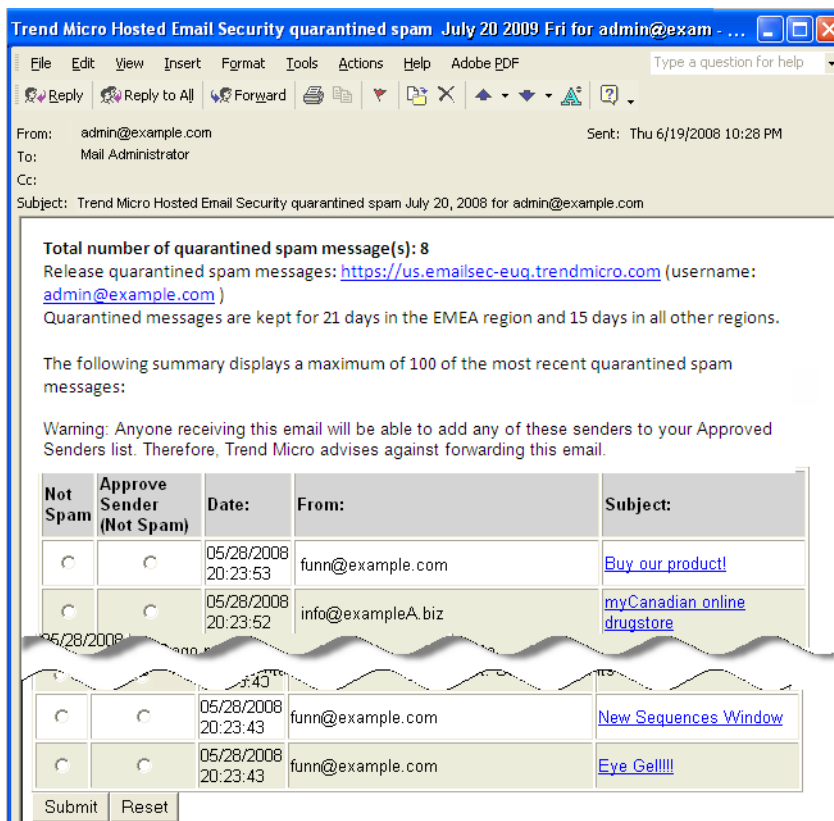



FIGURA 4-5. Messaggio e-mail Digest HTML di esempio con l'azione incorporata abilitata (troncata per leggibilità)

Servizio Web End-User Quarantine

Hosted Email Security Web End-User Quarantine (EUQ) consente agli utenti finali di:

- Creare un nuovo account
- Configurare azioni anti-spam con messa in quarantena e un elenco dei mittenti approvati
- Modifica delle password

Gli utenti finali possono accedere all'Hosted Email Security Web EUQ al seguente URL.

Per gli utenti residenti in Europa, Medio Oriente e Africa (EMEA):

http://emailsec-euq.trendmicro.eu

Per gli utenti residenti negli Stati Uniti e nelle aree che non rientrano nel gruppo EMEA:

https://us.emailsec-euq.trendmicro.com

Per ulteriori informazioni su Hosted Email Security Web EUQ, consultare la sezione *Introduzione a Web EUQ* a pagina C-1, la Guida in linea di Web EUQ o la Guida per gli utenti finali di *Hosted Email Security Web EUQ*.

Reimpostazione della password utente finale

Gli amministratori di sistema possono inviare agli utenti finali che abbiano dimenticato la password il link Password dimenticata della pagina Hosted Email Security Web EUQ necessario a reimpostarla. Gli utenti finali che devono reimpostare la password devono rispondere alla domanda di sicurezza inserita al momento della creazione dell'account.

Se gli utenti hanno dimenticato la domanda di sicurezza, gli amministratori di sistema sono in grado di reimpostare le password degli utenti finali. Quando un amministratore di sistema reimposta la password di un utente finale, attiva automaticamente anche l'account. L'utente finale che reimposta la password riceve subito un messaggio e-mail di autenticazione che consente l'accesso al servizio Web EUQ.

Registri

La sezione Registri consente di cercare e visualizzare i registri di verifica posta in base a: intervallo di date, data specifica, mittente, direzione (in entrata e in uscita) o destinatario. Le informazioni della verifica posta sono disponibili solo per i sette giorni precedenti.

FIGURA 4-6. Schermata Verifica posta che mostra i risultati delle query per il traffico in entrata

Dettagli della verifica posta

Nella schermata Verifica posta, è possibile individuare i messaggi presenti nel sistema utilizzando le informazioni su mittente e destinatario.Gli utenti di Hosted Email Security possono creare query nella posta in entrata e in uscita. La tabella dei risultati mostra lo stato e l'azione eseguita sul messaggio come:

- Bloccato o ritardato a margine del sistema dal servizio di reputazione (per la posta in entrata) o dal sistema di posta relay di Hosted Email Security (per la posta in uscita)
- Accettato per l'elaborazione ed eliminato con un virus
- Accettato, elaborato e recapitato
- Non risolto

È inoltre possibile cercare anche i messaggi e-mail inviati utilizzando Transport Layer Security (TLS). Se viene visualizzata l'icona TLS, ciò potrebbe indicare che Hosted Email Security ha accettato/consegnato il traffico di posta da o all'MTA downstream tramite TLS.

Verificato il	Componente	Tipo di evento	Dettagli	Upstream	Downstream
09/07/12 15.49.13	Inbound MTA	Delivered	250 2.0.0 Ok: queued as ECF197A3035		Scanner
09/07/12 15.49.13	Scanner	Delivered		Inbound MTA	Outbound MTA
09/07/12 15.49.14	Outbound MTA	Delivered	250	Scanner	

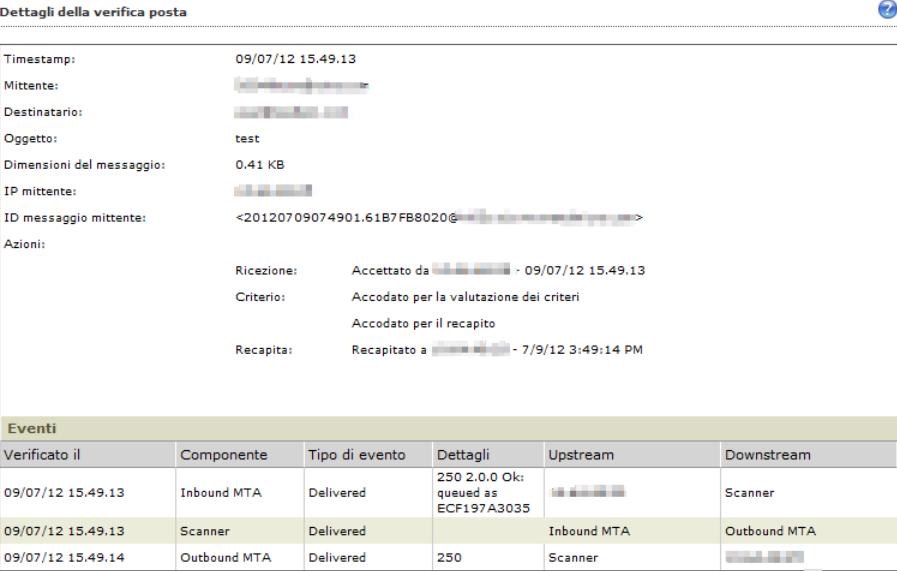
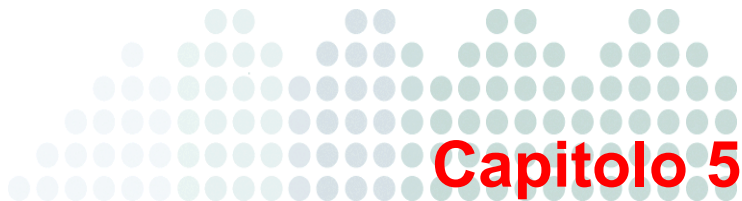



FIGURA 4-7. Dettaglio degli eventi nella pagina Verifica posta

Facendo clic sulla data di una voce di registro sarà possibile visualizzare la schermata Dettagli della verifica posta con ulteriori informazioni relative al messaggio.

I campi utilizzati per classificare ciascun registro di verifica dei messaggi sono descritti di seguito:

TABELLA 4-2. Dettagli della verifica messaggi

CAMPO	DESCRIZIONE
Data e ora	Data e ora in cui il messaggio è stato accettato.
Mittente	Indirizzo e-mail del mittente.
Destinatario	Indirizzo e-mail del destinatario. Se il messaggio contiene più destinatari, viene indicato solo il destinatario specifico della copia corrente del messaggio.
Oggetto	L'oggetto del messaggio, esclusi eventuali timbri inseriti.
Dimensioni del messaggio	La dimensione totale del messaggio e di tutti gli allegati.
IP mittente	Indirizzo IP del server di origine del mittente.
ID messaggio mittente	ID messaggio mostrato nel campo ID messaggio: dell'intestazione dell'e-mail. In genere si tratta dell'ID messaggio creato dal client di posta del mittente in cui è stato originato il messaggio.
Azioni	Azioni attivate dal messaggio. Vengono raggruppate in tre gruppi: ricezione, criteri e consegna.
Eventi	Questa sezione descrive il flusso di messaggi attuale. Vengono fornite le informazioni seguenti: Verificato: data e ora del momento in cui si è verificato il tipo di evento. Componente: il componente di messaggistica che ha elaborato l'evento. Tipo di evento: Azione finale per questo processo specifico. I tipi di eventi sono: Recapitato, Ritornato al mittente, Scaduto, Eliminato, In quarantena, Reindirizzato, Recapita subito, Accodato per il recapito, Crittografia in corso, Crittografato e Impossibile crittografare Dettagli: descrizione del flusso dei messaggi. A monte/A valle: la trasmissione da un componente/origine al successivo.

Amministrazione e reputazione IP

Questo capitolo fornisce informazioni sulla configurazione delle impostazioni di reputazione IP e su diverse attività di amministrazione accessibili dal menu Amministrazione.

Gli argomenti trattati nel presente capitolo includono:

Impostazioni di reputazione IP

Hosted Email Security può utilizzare le funzionalità di reputazione IP di Trend Micro Email Reputation Services (ERS) come servizio Trend Micro separato. Per accedere a questi servizi, fare clic su **Reputazione IP** sul menu a sinistra.

È possibile utilizzare la barra di scorrimento di reputazione dinamica per regolare l'aggressività del blocco delle connessioni e-mail da parte di ERS. È anche possibile scegliere il livello di aggressività del blocco dei server di posta ad alto volume, come descritto in *Regolazione delle impostazioni di esclusione IP* a pagina 5-4.

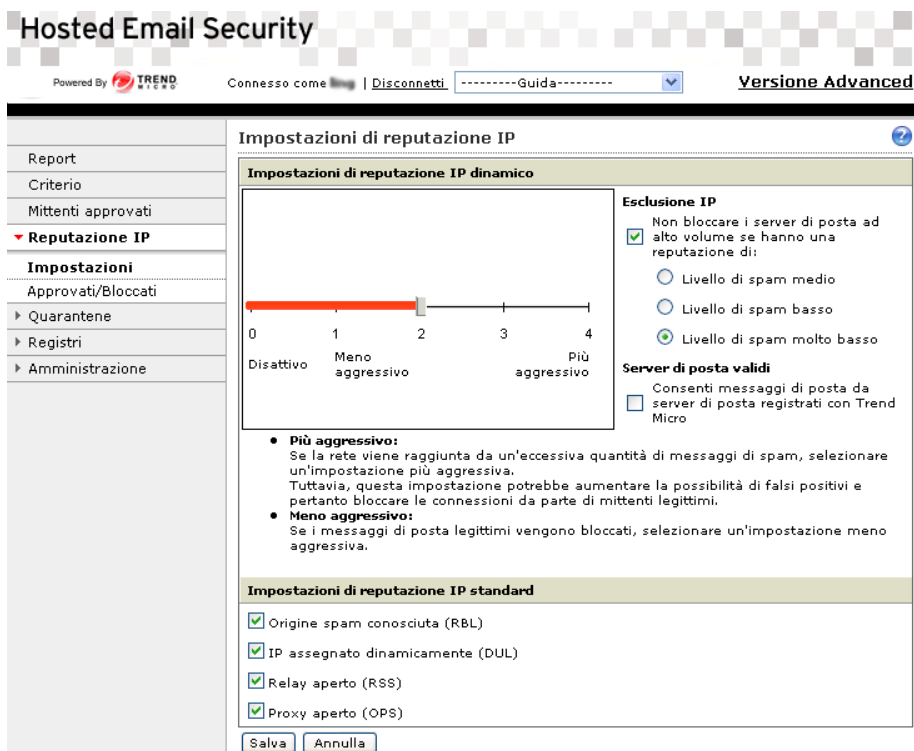



FIGURA 5-1. Schermata Impostazioni di reputazione IP

Utilizzo della barra di scorrimento di reputazione dinamica

È possibile utilizzare la barra di scorrimento di reputazione dinamica per impostare livelli di blocco nel seguente modo:

- **Più aggressivo:** se la propria rete viene raggiunta da un'eccessiva quantità di messaggi di spam, selezionare un'impostazione più aggressiva. Tuttavia, questa impostazione potrebbe aumentare la possibilità di falsi positivi e pertanto bloccare le connessioni da parte di mittenti legittimi.
- **Meno aggressivo:** se vengono bloccati messaggi di posta legittimi, selezionare un'impostazione meno aggressiva.

Suggerimento: Trend Micro consiglia di apportare modifiche alle impostazioni dinamiche con cautela e a piccoli incrementi. È possibile quindi regolare le impostazioni in base all'aumentata quantità di spam e ai messaggi legittimi ricevuti.

Per regolare le impostazioni di reputazione dinamica:

1. Dal menu a sinistra, selezionare **Reputazione IP**. Viene visualizzata la schermata Impostazioni di reputazione IP.
2. Spostare la barra di scorrimento su uno dei seguenti punti:

   Livello 4: l'impostazione più aggressiva. Se ERS (Email Reputation Services) rileva anche un singolo messaggio di spam da un indirizzo IP mittente, aggiunge l'indirizzo del mittente nel database di reputazione dinamica. La quantità di tempo in cui l'indirizzo IP rimane nel database dipende dal rilevamento di ulteriori messaggi di spam dal mittente.

   Livello 3: impostazione moderatamente aggressiva. ERS consente un ridotto volume di spam dai mittenti con una buona classificazione. Tuttavia, se ERS rileva un aumento di spam oltre il limite consentito da tale mittente, aggiunge questo mittente al database di reputazione dinamica. La quantità di tempo in cui l'indirizzo IP rimane nel database dipende dal rilevamento di ulteriori messaggi di spam dal mittente. La durata può essere estesa fino al valore massimo del livello 4.

   Livello 2: impostazione moderatamente tollerante. ERS consente un volume più ampio di spam da un mittente con una buona classificazione. Tuttavia, se ERS rileva un aumento di spam al di sotto del limite consentito da tale mittente, aggiunge questo mittente al database di reputazione dinamica. La quantità di tempo in cui l'indirizzo IP rimane nel database è in genere inferiore rispetto a quella del livello 3.

Livello 1: l'impostazione meno aggressiva. ERS consente la stessa quantità di spam da un mittente con una buona classificazione rispetto a quella del livello 2. La quantità di tempo in cui l'indirizzo IP rimane nel database è in genere inferiore rispetto a quella del livello 2.

Livello 0: effettua query al database di reputazione dinamica, ma non blocca gli indirizzi IP.

3. Fare clic su **Salva**.

Nota: L'impostazione predefinita è il livello 2, ovvero un'impostazione moderatamente tollerante.

Regolazione delle impostazioni di esclusione IP

I server di posta ad alto volume possono inviare una quantità di posta molto elevata, una parte della quale è sicuramente spam. Un server di posta ad alto volume (solitamente nel caso di un ISP di grandi dimensioni) può inviare un numero abbastanza elevato di messaggi di spam per i quali ERS (Email Reputation Services) inserisce l'IP del server di posta in un elenco di blocco. Tuttavia, è possibile impedire a ERS di bloccare il server di posta ad alto volume, grazie alla possibilità di bloccare l'eccessiva quantità di messaggi legittimi.

Oltre a regolare l'aggressività generale delle impostazioni di reputazione utilizzando la barra di scorrimento di reputazione dinamica, è possibile impostare ERS per il blocco dei server di posta ad alto volume che presentano un livello di reputazione medio, basso o molto basso.

Sezione Esclusione IP

Le impostazioni di esclusione IP operano congiuntamente all'impostazione della barra di scorrimento di reputazione dinamica a sinistra. Per disabilitare questa funzione, deselezionare la casella di controllo accanto a **Non bloccare i server di posta ad alto volume (ad esempio, gli ISP) se hanno una reputazione di**.

Per selezionare un livello di esclusione per i server di posta ad alto volume:

1. Nella schermata Impostazioni di reputazione IP, a destra della sezione Impostazioni dinamiche, accertarsi che la casella di controllo accanto a **Non bloccare i server di posta ad alto volume (ad esempio, gli ISP) se hanno una reputazione di** sia selezionata (valore predefinito), quindi selezionare una delle seguenti opzioni:
   - Livello di spam medio
   - Livello di spam basso
   - Livello di spam molto basso (impostazione predefinita)
2. Fare clic su **Salva**. ERS escluderà dal blocco automatico i server di posta ad alto volume che soddisfano l'opzione selezionata.

Server di posta validi

Se si seleziona questa casella di controllo, ERS consentirà le connessioni da tutti i server di posta designati come "Server di posta validi", a prescindere dal fatto che possano inviare o meno messaggi di spam. Questo elenco si basa sull'invio degli MTA da parte degli utenti.

Selezione degli elenchi di reputazione di IP standard

È possibile scegliere gli elenchi da abilitare tra quelli che costituiscono il database di reputazione e-mail standard. Per impostazioni predefinita, sono abilitati tutti gli elenchi. L'impostazione predefinita è la combinazione più efficace per la riduzione dei livelli di spam, che soddisfa le esigenze della maggior parte degli utenti.

ATTENZIONE! **Se si disabilitano alcune parti del database di reputazione IP standard, potrebbe verificarsi un aumento dei messaggi di spam che raggiungono il server di posta interno per un ulteriore filtraggio del contenuto.**

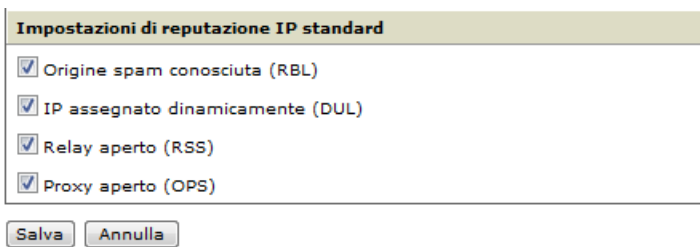



FIGURA 5-2. Per impostazione predefinita, sono selezionati tutti e quattro gli elenchi di reputazione IP standard.

Il database di reputazione IP standard comprende i seguenti quattro elenchi:

- **RBL (Real-time Blackhole List)** è un elenco di indirizzi IP di server di posta che sono noti come origini di spam.
- **DUL (Dynamic User List)** è un elenco di indirizzi IP assegnati dinamicamente oppure di quelli con un criterio di utilizzo accettabile che proibisce i server di posta pubblici. La maggior parte delle voci viene gestita in cooperazione con l'ISP proprietario dello spazio di rete. Gli indirizzi IP in questo elenco non dovrebbero inviare direttamente i messaggi e-mail, ma utilizzare piuttosto i server di posta del rispettivo ISP.
- **RSS (Relay Spam Stopper)** è un elenco di indirizzi IP di server di posta che sono relay di posta aperti e origini di spam note. Un relay di posta aperto è un server che accetta posta da qualsiasi utente su Internet indirizzata a qualsiasi altro utente su Internet, rendendo in questo modo difficile o impossibile tenere traccia degli spammer.
- **OPS (Open Proxy Stopper)** è un elenco di indirizzi IP di server che sono proxy aperti e origini di spam note. Un server proxy aperto è un server che accetta le connessioni da qualsiasi utente su Internet e che agisce da relay dei messaggi provenienti da tali connessioni verso qualsiasi server su Internet, rendendo in questo modo difficile o impossibile tenere traccia degli spammer.

Elenco Approvati e Bloccati per reputazione IP

Gli elenchi Approvati e Bloccati per la reputazione IP, visualizzati in *figura 5-4* a pagina 5-9 consentono di ricevere i messaggi provenienti dai paesi, dagli ISP, dagli indirizzi IP o dagli intervalli CIDR inclusi nell'elenco, ignorando il filtro a livello IP. Gli elenchi Approvati e Bloccati vengono applicati al proprio account Hosted Email Security, non all'MTA; è tuttavia possibile configurare altri elenchi di mittenti attendibili o bloccati o applicare filtri addizionali all'MTA.

La possibilità di ignorare il filtro IP richiede risorse aggiuntive per l'elaborazione, l'applicazione del filtro e l'archiviazione dei messaggi spam di livello più elevato che sarebbero altrimenti bloccati. Quando si utilizzano gli elenchi Approvati e Bloccati è possibile che i tassi di intercettazione spam globali risultino inferiori.

Nota: Gli elenchi Approvati per reputazione IP sono diversi dall'elenco di mittenti approvati generico che si trovano sul primo livello del menu sulla sinistra. La schermata si riferisce esclusivamente alle verifiche della reputazione IP; nella schermata dei mittenti approvati generica è possibile invece configurare indirizzi e-mail o domini aggiuntivi in modo che non vengano sottoposti ad alcuna scansione da parte di Hosted Email Security.

Blocca tutti i paesi ad eccezione di

Nella scheda Bloccati è presente una funzione non presente nella scheda Approvati. È possibile scegliere di bloccare tutti i paesi ad eccezione di determinati paesi inclusi in un elenco, come mostrato nella *figura 5-3*.

FIGURA 5-3. Schermata degli elenchi Approvati e Bloccati con la funzione Blocca tutti i paesi ad eccezione di

Utilizzando tale funzione, è possibile configurare Hosted Email Security per il blocco dei messaggi e-mail da tutti i paesi ad eccezione di quelli inclusi nell’elenco di paesi approvati dall’organizzazione.

In caso di ricerca del servizio reputazione standard (RBL), la gerarchia di valutazione è la seguente.

1. IP approvato
2. IP bloccato
3. ISP o ASN approvati
4. ISP o ASN approvati
5. Paese approvato
6. Paese bloccato

Per una ricerca del servizio di reputazione dinamica (QIL), gli elenchi di criteri bloccati (IP, ISP/ASN, Paese) vengono ignorati e vengono verificati solo gli elenchi Approvati. In caso contrario, l'ordine dei criteri di ricerca (prima IP, quindi ISP/ASN e infine Paese) è lo stesso di quello del servizio di reputazione standard (RBL).

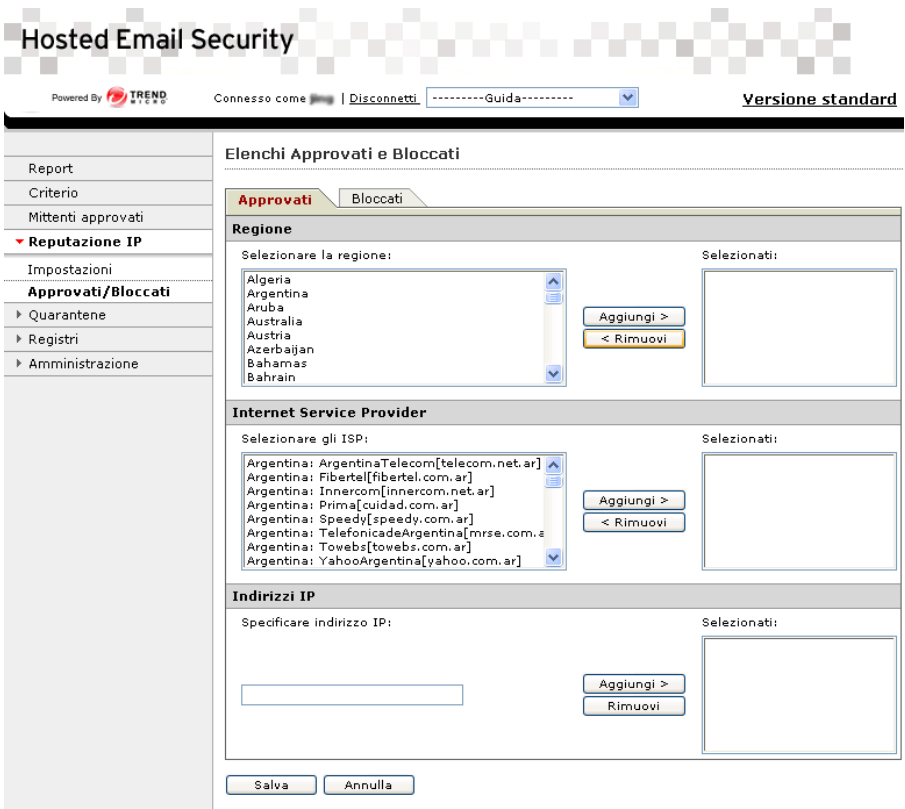



FIGURA 5-4. Schermata degli elenchi Approvati e Bloccati per reputazione IP

Risoluzione dei problemi relativi alle impostazioni di reputazione IP

Eventuali errori imprevisti che si verificano mentre si usa la schermata Reputazione IP possono essere risolti facilmente senza ricorrere all'assistenza tecnica. Prima di rivolgersi all'assistenza tecnica, consultare la *tabella 5-1* che segue per informazioni su come risolvere il problema.

TABELLA 5-1. Guida per la risoluzione dei problemi relativi alla schermata Impostazioni di reputazione IP

PROBLEMA	CAUSA POSSIBILE	SOLUZIONE POSSIBILE
IL PULSANTE SALVA È DISABILITATO.	Manca il codice di attivazione.	Richiedere al proprio fornitore un codice di attivazione valido.
	Il codice di attivazione è stato richiesto, ma non è stato ancora aggiunto al sistema Hosted Email Security.	Riprovare dopo un paio d'ore.
	Un problema di rete temporaneo impedisce a Hosted Email Security di convalidare il codice di attivazione.	Riprovare dopo qualche minuto.
IMPOSSIBILE SALVARE LE PROPRIE IMPOSTAZIONI DI REPUTAZIONE IP.	Si è verificato un problema di rete temporaneo.	• Riprovare dopo qualche minuto. • Disconnettersi, quindi connettersi nuovamente.
	Sono state aperte più finestre del browser contenenti la schermata Reputazione IP del sito Hosted Email Security e la sessione nella finestra che è stata aperta per prima è scaduta.	Passare alla finestra aperta per ultima e chiudere l'altra.

Amministrazione

Nella sezione Amministrazione, è possibile trovare i collegamenti alle schermate relative ai seguenti argomenti:

- *Modifica della password amministratore* a pagina 5-12
- *Reimpostazione password utente finale per Web EUQ* a pagina 5-13
- *Gestione delle directory* a pagina 5-13
- *Gestione dei domini* a pagina 5-17
- *Co-branding* a pagina 5-22
- *Servizi Web* a pagina 5-28
- *Visualizzazione del Contratto sul livello dei servizi* a pagina 5-30
- *Gestione remota* a pagina 5-32

Modifica delle password

Gli amministratori possono modificare la password amministratore e reimpostare una password dimenticata per un utente finale che deve accedere al servizio Hosted Email Security Web End-User Quarantine (EUQ).

Tutte le password Hosted Email Security devono avere una lunghezza compresa tra 8 e 32 caratteri. Trend Micro consiglia vivamente di utilizzare password contenenti più tipi di caratteri (una combinazione di lettere, numeri e altri caratteri) non riconducibili a un formato riconoscibile (ad esempio, non utilizzare date di compleanno, le cifre della propria targa, ecc.).

FIGURA 5-5. Schermata Cambia password amministratore

Modifica della password amministratore

Per modificare la password amministratore:

1. Accedere a **Amministrazione > Password amministratore**.
2. Digitare la password vecchia/corrente.
3. Digitare la nuova password.
4. Confermare la nuova password.
5. Fare clic su **Salva**.

Reimpostazione password utente finale per Web EUQ

Gli amministratori di sistema possono reimpostare una password utente finale dimenticata.

Per reimpostare una password utente finale:

1. Fare clic su **Amministrazione > Password utente finale**.

FIGURA 5-6. Schermata modifica password utente finale

2. Immettere l'indirizzo e-mail dell'utente finale.
3. Immettere e confermare una nuova password.

Nota: Per effettuare l'accesso, è necessario conoscere la nuova password.

4. L'utente finale riceverà un messaggio e-mail con un URL di attivazione.

   L'utente finale deve fare clic sull'URL di attivazione e quindi immettere l'indirizzo e-mail appropriato e una nuova password nella schermata di accesso di Hosted Email Security Web EUQ.

Gestione delle directory

Hosted Email Security utilizza le directory per prevenire lo spam di tipo backscatter (o "outscatter") e gli attacchi Directory Harvest Attacks (DHA). L'importazione delle directory utente permette a Hosted Email Security di conoscere gli indirizzi e-mail e i domini legittimi dell'organizzazione. Hosted Email Security riconosce soltanto file nel formato LDAP Data Interchange Format con codifica ANSI (LDIF: .ldf) e file CSV (Comma Separated Values) ANSI o UTF-8 .

La schermata Gestione directory (Amministrazione > Gestione directory) contiene le seguenti sezioni:

- **Sezione Importa directory utente:** campi per l'importazione di un nuovo file di directory utenti.
- **Directory utente importate:** i file delle directory utenti attualmente utilizzati da Hosted Email Security. Hosted Email Security sostituisce un utente di dominio e-mail per volta. Gli utenti possono essere formati da una combinazione di più directory utente.

Note sulla gestione delle directory

Prima di importare un file di directory LDIF o CSV, tenere conto di quanto segue:

- È possibile visualizzare unicamente le directory associate al proprio account amministratore. Se si condivide il servizio Hosted Email Security con un altro amministratore, quest'ultimo non vedrà le directory per quell'account al momento dell'accesso.
- Ogni volta che si aggiungono utenti alla propria rete, è necessario importare le directory utenti aggiornate; in caso contrario, Hosted Email Security rifiuta i messaggi e-mail provenienti dagli utenti appena aggiunti.
- Non includere righe vuote o altri dati non necessari nel file da importare. Durante la creazione di un file, prestare la massima attenzione.
- Ogni volta che si importa un file di directory, esso sovrascrive la versione precedente.

  Tuttavia, se si importa un file di directory utenti aggiornato che non contiene informazioni per uno dei propri domini, le voci relative a tale dominio restano invariate per Hosted Email Security e non vengono quindi sovrascritte.

ATTENZIONE! **Durante l'importazione di un file di directory, procedere con cautela. Se si importa un file di directory aggiornato che contiene informazioni su uno dei propri domini, tutte le voci relative a tali domini vengono sovrascritte.**

Esportazione di un file di directory utenti

Per prima cosa, esportare le directory dal sistema in uso. Trend Micro consiglia di utilizzare lo strumento LDIFDE per creare un file LDIF. Per istruzioni sull'uso dello strumento LDIFDE e sulla creazione del file, visitare il seguente collegamento sul sito Web Microsoft: http://support.microsoft.com/kb/237677

Importazione di un file di directory utenti

ATTENZIONE! **Trend Micro consiglia vivamente di non importare più di 24 directory al giorno. L'importazione di un numero superiore di directory potrebbe sovraccaricare le risorse del sistema.**

Per importare un file di directory utenti:

1. Fare clic su **Amministrazione > Gestione directory**. Viene visualizzata la schermata Gestione directory.

FIGURA 5-7. Gestione directory, schermata

2. Dall'elenco a discesa **Formato**, selezionare il tipo di formato:
   - **LDIF**
   - **CSV**
3. Accanto al campo **Nome**, digitare un nome descrittivo per il file.
4. Nel campo **Percorso file**, immettere il percorso directory e il nome del file oppure fare clic su **Sfoglia** e selezionare il file .ldf o .csv sul computer.

5. Fare clic su **Verifica file**. Al completamento della barra di avanzamento, viene mostrata una schermata contenente i seguenti elementi:
   - **Riepilogo:** un riepilogo delle informazioni descritte sopra.
   - **Domini e numero di utenti correnti per la sostituzione degli utenti correnti:** domini specificati al momento dell'iscrizione al servizio Hosted Email Security.
   - **Domini non validi:** domini inclusi nel file di directory ma non ufficialmente utilizzati nel servizio Hosted Email Security. Hosted Email Security non può fornire il servizio per questi domini e per gli indirizzi e-mail corrispondenti.
6. Fare clic su **Importa**.

Verifica della directory di utenti

Se non si è certi dei domini delle directory utente che saranno attivi per il servizio in uso, è possibile disabilitare temporaneamente le directory, importare il file, esportare le directory in un file CSV e visualizzarle senza che la directory sia effettivamente attiva. Quando si ha la certezza che le directory utenti sono corrette, è possibile attivarle nuovamente.

Nota: Le directory contenute nel file vengono attivate per impostazione predefinita. Quando una directory è abilitata, nella tabella **Directory utenti importata** viene visualizzato un segno di spunta verde: . Quando è disabilitata, viene visualizzata una X rossa: . L'abilitazione o disabilitazione delle directory in Hosted Email Security richiede fino a 5 minuti.

Per verificare le directory utenti:

1. Disattivare le directory facendo clic sull'icona "abilitato" (). La casella di controllo diventa una X rossa di "disabilitato" () e viene visualizzata la parola **Disabilitato**.
2. Importare il file di directory (vedere *Per importare un file di directory utenti:* a pagina 5-15).
3. Selezionare il dominio da verificare.
4. Fare clic su **Esporta** e salvare il file directory localmente (in formato CSV).
5. Aprire il file delle directory in un'applicazione che legga i file CSV.
6. Verificare che le informazioni sulle directory siano corrette.
7. Abilitare di nuovo le directory facendo clic sull'icona "disabilitato" ().

Gestione dei domini

Invece di fornire i domini della propria azienda allassistenzatecnicadiTrendMicro'Hosted Email Security, per aggiungere, modificare o eliminare i domini è possibile usare la schermata Gestione dominio.

Informazioni sullo stato del dominio

Lo stato dei domini gestiti può essere uno dei seguenti:

- Normale: il dominio recapita correttamente i messaggi e-mail.
- Sospeso: il dominio non ha recapitato correttamente i messaggi e-mail negli ultimi 30 giorni.

  Hosted Email Security modifica lo stato in Normale quando si verifica una delle seguenti condizioni:

  - I messaggi e-mail vengono recapitati correttamente al dominio registrato
  - L'indirizzo IP del relay del dominio registrato viene modificato

  Inoltre, è possibile riattivare manualmente i domini sospesi (vedere pagina 5-22).
- Timbrato (periodo consentito): il dominio non ha recapitato correttamente i messaggi e-mail negli ultimi 5 mesi.

  Quando un dominio è in questo stato (ovvero manca solo un mese all'interruzione completa del dominio), Hosted Email Security crea un criterio globale per i domini con lo stato SOSPESO. Hosted Email Security timbra ogni messaggio e-mail consegnato a quel dominio come promemoria che se non viene intrapresa alcuna azione, il dominio verrà interrotto. Se un dominio viene riattivato, il timbro viene rimosso insieme al criterio globale corrispondente.
- Interrotto: il dominio viene sospeso per almeno sei mesi; il traffico di relay è stato inesistente negli ultimi 30 giorni.

  Quando un dominio viene interrotto, non è più possibile riattivare il servizio o modificarne lo stato.

  L'interruzione di un server disattiva in modo permanente il dominio e impedisce l'indirizzamento dei messaggi e-mail da Hosted Email Security verso quel server. Hosted Email Security analizza e cancella i record MX indirizzati al servizio per impedire loop di posta.

  Quando un server è interrotto, qualunque record MX supplementare per quel dominio viene rimosso. Tale operazione impedisce il loop della posta. Di conseguenza, tale funzione rimuove statistiche imprecise sui domini gestiti e impedisce l'attivazione di criteri errati.

Aggiunta di un dominio

Per aggiungere un nuovo dominio:

1. Selezionare **Amministrazione > Gestione dominio** per aprire la schermata Gestione dominio, come mostrato nella *figura 5-8* che segue.

FIGURA 5-8. Schermata Gestione dominio di Hosted Email Security, come visualizzata all'accesso o con l'utilizzo di un account OLR

2. Inserire le seguenti informazioni nei campi forniti (i campi obbligatori sono mostrati in grassetto):
   - Nu ovonome **dominio**
   - Numero di **postazioni assegnate** a questo dominio

     Le postazioni corrispondono al numero di utenti e-mail effettivi nel dominio.
   - **Indirizzo IP/FQDN** (fully qualified domain name) e numero di preferenza del server di destinazione

     È possibile specificare fino a 30 server di destinazione per il traffico in entrata. Inoltre, il valore di preferenza può essere compreso tra 1 e 100.

     Nota: Se sono presenti più server di destinazione in un dominio del destinatario, MTA seleziona il server di destinazione con il numero di preferenza minimo. Di conseguenza, se sono presenti due o più server di destinazione con lo stesso numero di preferenza, MTA seleziona casualmente uno di essi come agent MTA a valle.

   - **Numero porta** del server di posta di destinazione
   - Account e-mail di prova

     Utilizzare questo indirizzo e-mail come destinatario dei messaggi di prova per confermarne il recapito mediante Hosted Email Security.
3. Selezionare **Attivazione filtro posta in uscita** e fornire l'indirizzo IP dei server posta in uscita. È possibile specificare fino a 30 indirizzi IP relay.
4. Fare clic su **Attiva dominio**.

Se il dominio è valido ed esiste un record MX (originale, non modificato) per il dominio, vengono visualizzati il nuovo dominio, l'indirizzo IP o l'FQDN, il numero porta, le postazioni e altre informazioni nella tabella Domini nella parte inferiore della schermata e Hosted Email Security invia un messaggio e-mail di conferma all'indirizzo e-mail di amministrazione nel record.

Nota: Il messaggio e-mail di conferma inviato da Hosted Email Security comunica se il dominio è stato aggiunto correttamente. Il completamento del processo di aggiunta del dominio potrebbe richiedere 24-48 ore.

Per aggiungere immediatamente il dominio all'elenco dei domini:

1. Attendere l'e-mail di conferma da Hosted Email Security.

ATTENZIONE! **Non modificare il record MX prima di ricevere l'e-mail di conferma.**

---

2. Modificare il record MX per includere il dominio.
3. Selezionare **Amministrazione > Gestione dominio** per aprire la schermata Gestione dominio.
4. Selezionare i domini aggiunti nell'elenco dei domini. Lo stato del dominio sarà "Verifica in corso".
5. Fare clic su **Verifica record MX** per verificare che il record MX del dominio punti al server Hosted Email Security Inbound MTA.

Nota: Se non si attiva un nuovo dominio e lo stato visualizzato continua a essere "Verifica in corso", controllare il record MX per il dominio. Accertarsi che il record MX punti all' Hosted Email Security FQDN corretto.

Conferma del recapito posta mediante il servizio

Al momento di aggiungere un dominio a Hosted Email Security, assicurarsi di inserire un indirizzo e-mail di prova, come citato in *Passaggio 2* in *Aggiunta di un dominio*. Dopo aver aggiunto il dominio ma prima di reindirizzare al record MX, inviare un messaggio e-mail di prova all'account di posta inserito e confermare che la posta passa liberamente attraverso Hosted Email Security. Se non si riceve il messaggio di prova, contattare il provider di servizi.

ATTENZIONE! **Non modificare il record MX prima di ricevere l'e-mail di conferma.**

Modifica di un dominio

È possibile modificare le informazioni del dominio nella schermata **Gestione dominio > {nome del dominio}**, a cui è possibile accedere facendo clic sul nome del dominio nella tabella Domini nella parte inferiore della schermata. Per questa schermata, vedere le *figura 5-9*.

Per modificare un dominio:

1. Selezionare **Amministrazione > Gestione dominio** dal menu a sinistra per aprire la schermata Gestione dominio, come visualizzato in *figura 5-8*.
2. Fare clic sul nome del dominio nella tabella situata nella parte inferiore della schermata Gestione dominio. Viene visualizzata la schermata **Gestione dominio > {nome del dominio}** con le informazioni per quel dominio presenti nei record già preimpostate nei relativi campi.
3. Modificare le informazioni desiderate, quindi fare clic su **Salva**.

FIGURA 5-9. Modifica informazioni del dominio nella schermata Gestione dominio > {dominio} (scrivibile solo quando è stato eseguito l’accesso con account OLR)

Nella schermata Gestione dominio è possibile disattivare un dominio.

Per disattivare un dominio:

1. Selezionare **Amministrazione > Gestione dominio** dal menu a sinistra per aprire la schermata Gestione dominio, come visualizzato in *figura 5-8*.
2. Selezionare la casella di controllo accanto al dominio da disattivare.
3. Fare clic sul collegamento **Disattiva** nell'intestazione o nel piè di pagina della tabella. La richiesta di disattivazione viene inoltrata a Trend Micro.

Riattivazione dei domini sospesi

Utilizzare la schermata Gestione dominio per impedire l'interruzione dei domini sospesi.

Per riattivare un dominio sospeso:

1. Selezionare **Amministrazione** > **Gestione dominio** dal menu a sinistra per aprire la schermata Gestione dominio.

   In alternativa, dopo aver effettuato l'accesso, fare clic sul collegamento Sospeso per essere reindirizzati alla schermata Gestione dominio.

2. Selezionare la casella di controllo accanto al dominio da riattivare.
3. Fare clic sul collegamento **Riprendi** nell'intestazione o nel piè di pagina della tabella. La richiesta di disattivazione viene inoltrata a Trend Micro.

Co-branding

Hosted Email Security consente di visualizzare il logo della propria società sul banner superiore della console Web e nella pagina di accesso.

I rivenditori possono impostare per il co-branding la console di amministrazione di Hosted Email Security, l'interfaccia Web EUQ o entrambe. I rivenditori possono impostare vari domini con lo stesso logo o con loghi diversi o consentire agli amministratori di dominio di impostare il logo da visualizzare nel loro dominio. In alternativa, possono lasciare la funzione disabilitata.

Specifiche del logo

Prima di impostare il co-branding per un sito, verificare che l'immagine del logo rispetti i seguenti requisiti:

- **Altezza immagine:** esattamente 60 pixel (né più alta né più bassa)
- **Larghezza immagine:** 800 – 1.680 pixel
- **Formato file immagine:** .gif, .jpg o .png

Co-branding della console di amministrazione

1. Fare clic su **Amministrazione > Co-branding.** Viene visualizzata la schermata Co-branding, come mostrato nella *figura 5-10*.
2. Fare clic sull'icona "Disabilitata" (Disattivato) situata nell'angolo in alto a destra per attivare la funzione. L'icona cambia in "Abilitata" (Enabled).

Nota: La funzione di co-branding è disabilitata per impostazione predefinita.

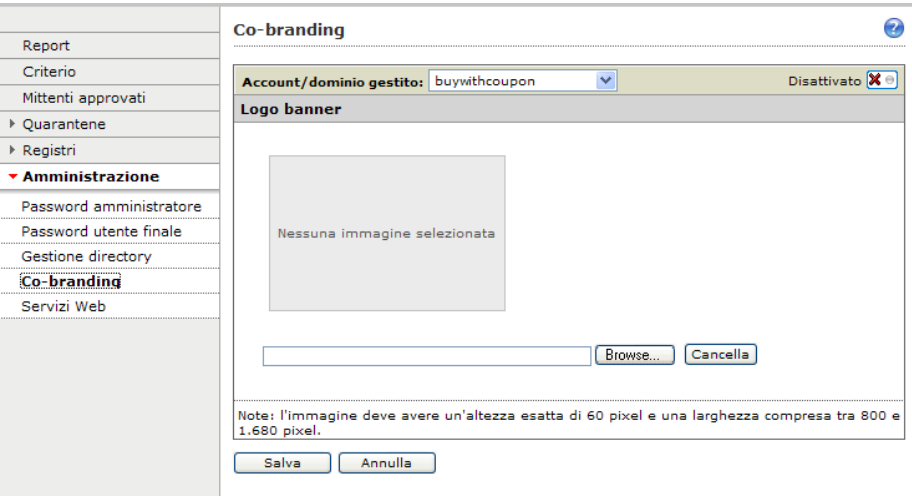



FIGURA 5-10. Pagina del co-branding

3. Dall'elenco a discesa **Account/Dominio gestito**, selezionare il nome dell'account che conterrà il logo, come mostrato nella *figura 5-11* che segue.

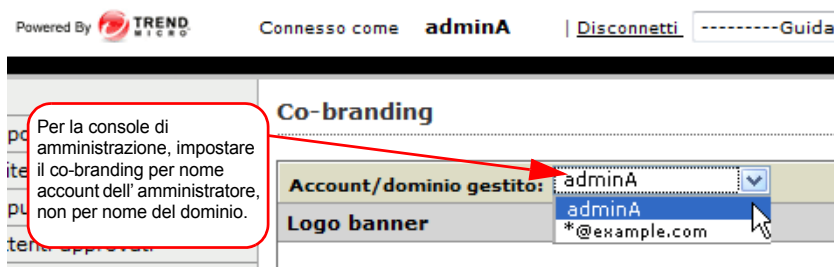



FIGURA 5-11. Co-branding della console di amministrazione (selezionare il nome dell'account, non il nome del dominio)

4. Fare clic su **Sfoglia** e selezionare il percorso del file del logo (per rimuovere il logo, fare clic su **Cancella**).
5. Fare clic su **Apri**; verrà visualizzata un'anteprima del logo, come mostrato nella *figura 5-12*.

FIGURA 5-12. Visualizzazione del logo di dominio da impostare

6. Fare clic su **Salva**. L'immagine del logo verrà visualizzata nel banner superiore della console di amministrazione Hosted Email Security (vedere la *figura 5-14*) e nella pagina di accesso come descritto in *Accesso a un sito in co-branding* a pagina 5-27.

Co-branding dell'interfaccia EUQ Web

I rivenditori possono impostare il co-branding anche per l'interfaccia EUQ Web. La procedura è quasi identica a quella utilizzata per definire una versione di co-branding della console di amministrazione Hosted Email Security con una piccola eccezione, descritta di seguito.

Per configurare una versione di co-branding dell'interfaccia EUQ Web:

1. Fare clic su **Amministrazione > Co-branding.** Viene visualizzata la schermata Co-branding, come mostrato nella *figura 5-10*.
2. Fare clic sull'icona "Disabilitata" (Disattivato) situata nell'angolo in alto a destra per attivare la funzione. L'icona cambia in "Abilitata" (Enabled).

Nota: La funzione di co-branding è disabilitata per impostazione predefinita.

3. Dall'elenco a discesa **Account/Dominio gestito**, selezionare il nome del dominio di cui si visualizzerà il logo, come mostrato nella *figura 5-13* che segue.

FIGURA 5-13. Co-branding dell'interfaccia EUQ Web (selezionare il nome del dominio, non il nome dell'account)

4. Fare clic su **Sfoglia** e selezionare il percorso del file del logo. (per rimuovere il logo, fare clic su **Cancella**).
5. Fare clic su **Apri**; verrà visualizzata un'anteprima del logo, come mostrato nella *figura 5-12*.
6. Fare clic su **Salva**. L'immagine del logo verrà visualizzata nel banner superiore dell'interfaccia Hosted Email Security EUQ Web e nella pagina di accesso EUQ (vedere la *figura 5-15*) come descritto in *Accesso a un sito in co-branding* a pagina 5-27.

Nota: I rivenditori possono impostare loghi diversi per domini diversi, o consentire agli amministratori di sistema del dominio di impostare il logo per il dominio separatamente rispetto al logo del rivenditore. Il logo selezionato per il nome account verrà visualizzato solo nella console di amministrazione Hosted Email Security. Il logo selezionato per un dominio verrà visualizzato solo nella barra del banner del modulo EUQ Web di Hosted Email Security associato a tale dominio.

FIGURA 5-14. Esempio di logo di rivenditore inserito nella barra del banner della schermata di accesso di Hosted Email Security

The ABCD Company
Powered By TREND MICRO
TREND MICRO
Hosted Email Security
Immettere l'indirizzo e-mail e la password per accedere alla console dei servizi.
Indirizzo e-mail:
user@example.com
Password:
Password dimenticata?
Registra un nuovo account
Accedi

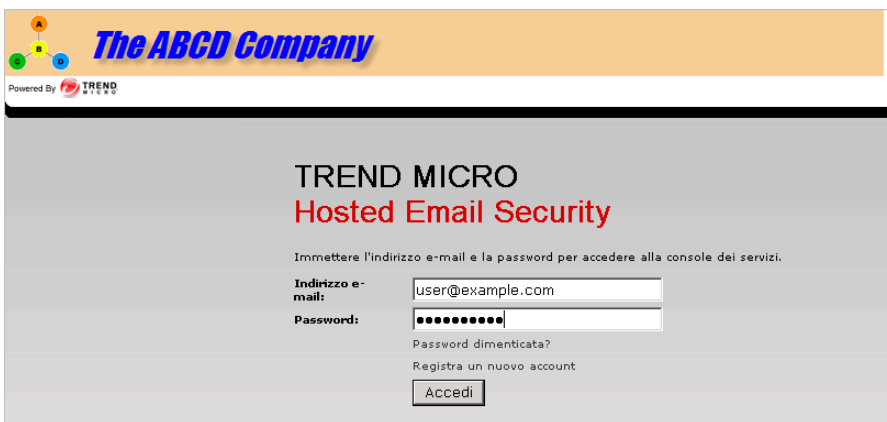



FIGURA 5-15. Il logo del dominio viene visualizzato nella barra del banner della schermata di accesso di Hosted Email Security Web EUQ

Accesso a un sito in co-branding

I rivenditori possono fornire ai clienti un indirizzo URL dal quale accedere al sito in co-branding.

Accesso a una console di amministrazione in co-branding

Sono disponibili diverse opzioni per l'accesso alla console di amministrazione in co-branding, a seconda del proprio tipo di accesso. Se l'account è stato registrato utilizzando il sito Web di Trend Micro Online Registration (OLR), aggiungere il nome account OLR Hosted Email Security e il co-branding all'URL di base.

Ad esempio, se "adminA" è il nome dell'account OLR Hosted Email Security, digitare quanto segue nella casella dell'indirizzo del browser:

"https://us.emailsec.trendmicro.com/**adminA/co-brand**"

Se l'account non è stato registrato mediante il sito Web di OLR, è ancora possibile accedere con le credenziali precedenti, aggiungendo il nome account Hosted Email Security originale all'URL di base come segue:

"https://us.emailsec.trendmicro.com/**adminA**"

Accesso a un sito EUQ Web in co-branding

Per accedere a un sito EUQ Web in co-branding, gli utenti finali aggiungono il nome del dominio alla fine dell'indirizzo URL di base:

"https://us.emailsec-euq.trendmicro.com"

Ad esempio, se "example.com" è il nome del dominio, gli utenti finali digiteranno quanto segue nella casella dell'indirizzo del browser:

"https://us.emailsec-euq.trendmicro.com/**esempio.com**"

Nota: Se un utente finale accede a un sito in co-branding senza aggiungere il nome dell'account o il nome del dominio, il sito verrà visualizzato e funzionerà regolarmente, ma senza co-branding.

Servizi Web

Hosted Email Security consente di accedere alle applicazioni dei Servizi Web Hosted Email Security tramite un client del Servizio Web Hosted Email Security installato nell'ambiente in uso.

Prima di accedere alle applicazioni dei Servizi Web Hosted Email Security è necessario compiere tre passaggi. È necessaria prima di tutto una chiave di autenticazione per il servizio. Tale chiave è l'identificatore univoco globale del client dei Servizi Web che consente di autenticarne l'accesso ai Servizi Web Hosted Email Security. Quindi, occorre attivare i Servizi Web Hosted Email Security. Infine, è necessario selezionare e installare il programma client dei Servizi Web nell'ambiente in uso.

Per preparare l'ambiente per i Servizi Web:

1. Fare clic su **Amministrazione > Servizi Web**

FIGURA 5-16. Schermata Servizi Web

2. Assicurarsi che sia disponibile una chiave di autenticazione per il servizio. Chiave corrente visualizza la chiave che il programma client dei Servizi Web deve utilizzare. Se si genera una nuova chiave, è necessario aggiornare il programma client per utilizzarla. La chiave di autenticazione per il servizio è come una password che consente al client di comunicare con i servizi Web Hosted Email Security. Fornire tale chiave esclusivamente agli amministratori Hosted Email Security autorizzati.

Nota: Se il campo **Chiave corrente** è vuoto, fare clic su **Genera nuova chiave** per generare una chiave di autenticazione per il servizio.

---

3. Fare clic sull'icona "disabilitato" (Disattivato) situata nell'angolo destro per attivare (Enabled) la funzione.

   Questa funzione è disabilitata per impostazione predefinita.
4. Dall'elenco **Download**, selezionare il programma client dei servizi Web Hosted Email Security da scaricare. Fare clic sull'icona () per scaricare il client.
5. Salvare il client sull'unità locale.
6. Seguire i passaggi per l'installazione del client.

Download della Guida ai servizi Web Hosted Email Security

Trend Micro ha preparato una guida per facilitare la comprensione e l'uso del servizio Web. È possibile scaricare la *Guida ai servizi Web* nella sezione Download della schermata Servizi Web, come mostrato nella *figura 5-17* a pagina 5-30.

Suggerimento: Trend Micro consiglia di scaricare e leggere la Guida ai servizi Web prima di procedere alla configurazione avanzata dei servizi Web.

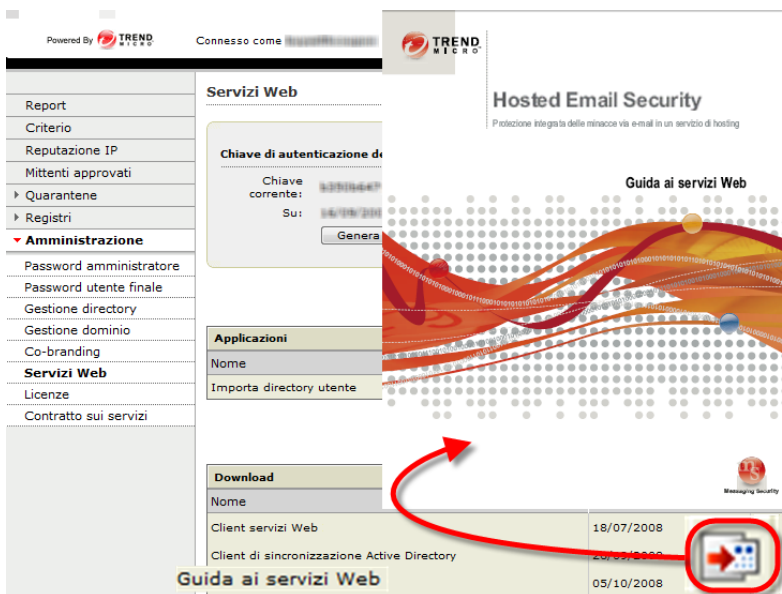



FIGURA 5-17. Scaricare la Guida ai servizi Web Hosted Email Security dalla sezione Download della schermata Servizi Web

Visualizzazione del Contratto sul livello dei servizi

Trend Micro fornisce un contratto sul livello dei servizi (SLA, Service Level Agreement) per Hosted Email Security che garantisce all'organizzazione la ricezione sicura e ininterrotta della posta elettronica per supportare le attività aziendali.

Questo contratto sul livello dei servizi copre la disponibilità, la latenza, il blocco dello spam, i falsi positivi, l'antivirus e l'assistenza tecnica. Le garanzie specifiche sul livello dei servizi sono incluse nell'ultima versione del contratto SLA Hosted Email Security, che è possibile visualizzare o scaricare dalla schermata Contratto sul livello dei servizi.

Nota: L termini del contratto SLA possono variare a seconda delle aree; pertanto, accertarsi di selezionare la lingua e l'area appropriate quando si utilizza questa schermata.

FIGURA 5-18. Schermata Contratto sul livello dei servizi Hosted Email Security

Per visualizzare il contratto SLA per la propria area:

1. Dal menu a sinistra, selezionare **Amministrazione > Contratto sui servizi**. Viene visualizzata la schermata Contratto sul livello dei servizi Hosted Email Security, come mostrato nella *figura 5-18*.

   Suggerimento: Per scaricare il contratto SLA, disabilitare eventuali blocchi di finestre a comparsa sul proprio browser.

2. Dall'elenco a discesa, selezionare la propria **lingua/regione.** Da Hosted Email Security viene aperta un'altra finestra del browser in cui viene visualizzato il documento Adobe Reader (PDF) relativo al contratto SLA della propria area, nella lingua selezionata.

Nota: Trend Micro si riserva il diritto di modificare il servizio in qualsiasi momento, senza preavviso. La versione corrente del contratto sul livello dei servizi Hosted Email Security è disponibile per la visione da parte dei clienti che hanno effettuato il pagamento e dei clienti che stanno effettuando una prova.

Gestione remota

È possibile utilizzare la schermata Delega gestione account, mostrata nella *figura 5-19*, per designare un utente che gestisca temporaneamente i criteri del proprio account Hosted Email Security. La funzionalità può essere utile per i rivenditori che gestiscono gli account di diversi utenti di Hosted Email Security. L'utente a cui è stata assegnata la capacità di gestione Hosted Email Security è in grado di visualizzare e regolare i criteri e le impostazioni Hosted Email Security utilizzando un prodotto Trend Micro specifico: Trend Micro Worry-Free Remote Manager (WFRM).

All'interno della console WFRM è presente un riepilogo delle impostazioni Hosted Email Security. Per gestire Hosted Email Security da WFRM, il rivenditore deve fare clic su un collegamento presente in WFRM che consente di aprire una finestra Hosted Email Security. Da tale finestra, è possibile effettuare qualsiasi modifica ai criteri che è possibile apportare dalla console di amministrazione Hosted Email Security. Vedere il sito Web Trend Micro per ulteriori informazioni su questo prodotto.

Per eseguire una delega, è necessario disporre della chiave di autorizzazione per il servizio che può essere ottenuta dal rivenditore il quale provvederà a generarla da WFRM.

FIGURA 5-19. Schermata Gestione remota (Delega gestione account) senza delega

Per delegare un utente alla gestione di un account in remoto, procedere come segue.

1. Nel menu di sinistra di Hosted Email Security, fare clic su **Amministrazione > Remote Manager**. Viene visualizzata la schermata Delega gestione account, come mostrato nella *figura 5-19* sopra riportata.
2. Digitare o incollare la chiave di autorizzazione del destinatario della delega della gestione e fare clic sul pulsante **Connetti.** Se il collegamento viene eseguito correttamente, la schermata verrà aggiornata mostrando il nome dell'account e la persona delegata, il suo indirizzo postale, di posta elettronica, il numero di telefono cellulare, la chiave contratto e la data di inizio della delega, come mostrato nella figura *figura 5-20* a pagina 5-33.

FIGURA 5-20. Gestione remota: gestione account delegata

È possibile annullare la delega in qualsiasi momento facendo clic su **Interrompi**.

Il delegato può a sua volta interrompere la delega da Worry Free Remote Manager. In caso di interruzione in remoto da parte del delegato, la schermata Delega gestione account mostra la maggior parte delle informazioni visualizzate nella versione "delegata" della schermata (mostrata nella *figura 5-20*) insieme al motivo dell'interruzione, come mostrato nella *figura 5-21*.

FIGURA 5-21. Schermata Delega gestione account dopo l'interruzione della delega da parte del delegato in remoto

Modalità di licenza

Allo scadere della licenza, si passa attraverso diverse modalità prima che sia completamente disattivata. Per capire le diverse modalità di licenza, vedere la tabella seguente.

TABELLA 5-2. Modalità di licenza

MODALITÀ DI LICENZA	DESCRIZIONE	LUNGHEZZA	STATO DI PROTEZIONE	OPERAZIONI DA ESEGUIRE
Attivo	La licenza è valida.	Normalmente un anno, a seconda dellabbonamento'	I domini sono protetti dal servizio.	Nessuno; rintracciare la data di scadenza della licenza.
Periodo consentito	La licenza è scaduta, ma rientra nel periodo consentito.	Normalmente un mese, a seconda dellabbonamento'	I domini sono protetti dal servizio. Viene inviata una notifica al proprietario della licenza registrato.	Rinnovare immediatamente la licenza.
Totalmente scaduta	Il periodo consentito è trascorso e la licenza è totalmente scaduta.	30 giorni	• Il servizio continua a filtrare i messaggi, ma inserisce un timbro nei messaggi in entrata con una notifica. I destinatari e-mail visualizzeranno questa notifica. • Laccessoalla'console di amministrazione è bloccato.	• Rinnovare immediatamente la licenza. • Contattare lassistenzatecnicaperdisabilitare'*temporaneamente* il timbro dai messaggi in entrata.

TABELLA 5-2. Modalità di licenza (segue)

MODALITÀ DI LICENZA	DESCRIZIONE	LUNGHEZZA	STATO DI PROTEZIONE	OPERAZIONI DA ESEGUIRE
Disattivato	Tutti i dati dellabbonamentovengonoeliminatipermanentemente.'	Permanente	• Tutti i dati relativi a dominio, criteri e posta vengono eliminati. • Tutti i messaggi in entrata vengono rifiutati (*codice di risposta 554*).	Richiedere una nuova licenza.

Appendice A

Domande frequenti

Le domande frequenti riportate di seguito sono relative alla versione corrente di Hosted Email Security

Domanda 1: Che cos'è Trend Micro™ Hosted Email Security?

Risposta: Trend Micro Hosted Email Security è un servizio di protezione dell'e-mail in hosting estremamente utile per aziende di tutte le dimensioni. Forniamo l'hardware, il software e la competenza nel campo della messaggistica per disinfettare i messaggi e-mail dagli attacchi tramite spam, virus, worm, cavalli di Troia e phishing (furto dell'identità). Il flusso disinfettato di messaggi e-mail viene inviato direttamente al server di posta per il recapito agli utenti finali.

Domanda 2: Quali sono i vantaggi offerti da un servizio di protezione dell'e-mail in hosting?

Risposta: Essendo un servizio di hosting esterno, Hosted Email Security è in grado di bloccare gli attacchi, prima che questi riescano a raggiungere la rete. Oltre a bloccare spam, virus, worm, cavalli di Troia e altre minacce, Hosted Email Security protegge la rete da attacchi che:

- Tentano di bloccare la connessione a Internet (Denial of Service)
- rubano indirizzi e-mail per gli spammer (Directory Harvest Attacks)

Domanda 3: Devo acquistare/aggiornare hardware o software?

Risposta: Hosted Email Security è un servizio in hosting che rende superfluo l'acquisto di hardware o software aggiuntivo. Il servizio è gestito dai nostri professionisti della sicurezza, che sollevano il personale informatico dall'onere di installare, mantenere e regolare un sistema complesso di protezione della posta elettronica.

Domanda 4: Quanto costa il servizio?

Risposta: Il prezzo di Trend Micro Hosted Email Security viene fissato per ogni utente su base contrattuale annua. I costi per utente diminuiscono in proporzione all'aumento del numero di utenti. Trend Micro non applica tariffe di impostazione o costi di assistenza aggiuntivi. Sebbene poco probabile, l'azienda che fornisce l'hosting Web potrebbe addebitare costi di lieve entità per la modifica del record MX. Per esaminare i criteri dei prezzi, contattare il servizio di hosting Web.

Domanda 5: Qual è il grado di riservatezza di questo servizio? (Voglio che nessuno legga la mia posta.)

Risposta: Tutti i messaggi vengono elaborati in modo automatico e trasparente. Molti messaggi vengono rifiutati prima ancora che vengano ricevuti sulla base della reputazione dell'IP che sta tentando di inviare il messaggio. I messaggi ricevuti vengono elaborati da un sistema di filtraggio antivirus e anti-spam a più livelli che non prevede interventi umani. I messaggi non vengono mai memorizzati a meno che il server di posta non diventi non disponibile.

Domanda 6: Perché dovrei fidarmi di Trend Micro per la gestione della mia posta elettronica?

Risposta: Trend Micro è un'azienda leader nella gestione delle minacce grazie a oltre 10 anni di esperienza nella prevenzione per messaggistica e spam e più di 25 anni nella fornitura di efficaci soluzioni antivirus. Negli ultimi 6 anni, Trend Micro ha detenuto la maggiore quota di mercato nel segmento delle soluzioni gateway Internet, mentre negli ultimi 4 anni si è affermata come la principale fornitrice di strumenti antivirus per server di posta. Conosciamo e comprendiamo appieno i problemi associati alla protezione delle reti da tutti i tipi di minaccia esistenti, veicolati o meno dai messaggi e-mail. Un gateway di messaggistica sicuro è uno dei componenti chiave di una soluzione di protezione della rete completa.

Domanda 7: Cosa serve per utilizzare questo servizio?

Risposta: Per utilizzare questo servizio è necessario solo un gateway Internet esistente o una connessione e-mail del gruppo di lavoro e un browser Web per accedere alla generazione di rapporti online e alla console di amministrazione.

Domanda 8: Come inizio a utilizzare il servizio? (Devo effettuare operazioni di installazione, configurazione o manutenzione?)

Risposta: Un semplice reindirizzamento del record Mail eXchange (MX) è tutto ciò che serve per avviare il servizio. Il messaggio e-mail viene elaborato da Trend Micro Hosted Email Security per rimuovere spam, virus, worm, cavalli di Troia e phishing; i messaggi sicuri vengono inviati direttamente al server di posta.

Domanda 9: Come posso reindirizzare il mio record e-mail/Mail eXchange?

Risposta: Se si può gestire il DNS, reindirizzare il record MX è molto semplice. Se invece il DNS è gestito da terzi o da un ISP, questi se ne occupano per conto dell'utente o approntano un'interfaccia Web intuitiva che consenta all'utente stesso di apportare le modifiche. Affinché le modifiche vengano propagate nel sistema, possono essere necessarie fino a 48 ore.

Per l'FQDN Hosted Email Security corretto, visitare la Trend Micro Knowledge Base all'indirizzo:

http://esupport.trendmicro.com

Domanda 10: Come accetto la posta dal servizio?

Risposta: Per accertarsi di poter ricevere i messaggi e-mail elaborati dal servizio:

- Configurare il firewall per accettare il traffico proveniente dagli Hosted Email Security indirizzi IP
- Configurare il server di posta per accettare le transazioni da questi indirizzi IP

Hosted Email Security Gli indirizzi IP possono cambiare. Per un elenco completo di indirizzi, visitare la Trend Micro Knowledge Base all'indirizzo:

http://esupport.trendmicro.com/Pages/How-to-accept-emails-coming-from-Hosted-Email-Security-servers-only.aspx

Domanda 11: Perché lo stato del mio dominio rimane su "Verifica in corso"?
Risposta: Quando si attiva un nuovo dominio, Hosted Email Security esegue diversi controlli e invia una e-mail di conferma. Quando si riceve questa e-mail, occorre modificare il record MX del dominio per puntare allFQDN'Hosted Email Security corretto. Se non si aggiorna il record MX del dominio, lo stato del dominio rimane su "Verifica in corso".

Per ulteriori informazioni, vedere *Gestione dei domini* a pagina 5-17.

Domanda 12: Posso provare il servizio su un numero limitato di utenti?
Risposta: Si consiglia di utilizzare un dominio di prova per eseguire il test. In questo modo si potrà provare il servizio e testarne le funzioni per diversi tipi di utenti.

Domanda 13: Questo servizio provocherà ritardi nella consegna del mio messaggio e-mail?
Risposta: Il tempo richiesto per elaborare ogni messaggio è nell'ordine di millisecondi. Qualsiasi ritardo nella consegna dei messaggi sarà trascurabile e l'utente non lo noterà nemmeno.

Domanda 14: I messaggi vengono memorizzati/archiviati da Trend Micro?
Risposta: Hosted Email Security non memorizza o archivia i messaggi per impostazione predefinita. Tutti i messaggi vengono elaborati e immediatamente passati all' MTA del cliente. Non si effettua lo spooling o la conservazione dei messaggi in memoria a meno, eccetto qualora il server di posta diventi non disponibile. Tuttavia, in caso di creazione di criteri per la quarantena dei messaggi e-mail (ad esempio lo spam), tali messaggi vengono memorizzati nel centro dati per un massimo di 21 giorni nella regione EMEA e 15 giorni in tutti gli altri paesi.

Domanda 15: Come si esegue il ripristino o un nuovo invio di una password utente finale di Web EUQ?
(Uno degli utenti ha perso o dimenticato la password.)
Risposta: Fare clic su **Amministrazione > Password utente finale** e compilare il modulo Modifica password utente finale. L'utente finale riceverà un messaggio e-mail contenente un URL di attivazione a cui dovrà accedere e quindi immettere l'indirizzo e-mail appropriato e una nuova password nella schermata di accesso di Hosted Email Security Web EUQ. Per ulteriori informazioni, vedere *Reimpostazione password utente finale per Web EUQ* a pagina 5-13.

Domanda 16: Cosa accade ai miei messaggi se il server di posta non è disponibile per un determinato lasso di tempo? (Vengono fornite soluzioni contro il Disaster Recovery?)

Risposta: Qualora il server di posta non dovesse essere disponibile per qualsiasi motivo, il flusso di messaggi verrà automaticamente messo in coda per cinque giorni o finché il server non tornerà online. Non si rischierà più di perdere importanti messaggi e-mail a causa di danni hardware o software, blackout, errore di rete o semplice errore umano.

Domanda 17: Dove finiscono i miei messaggi in uscita?

Risposta: Per impostazione predefinita, il flusso di posta in uscita viene gestito direttamente dal server di posta e passa alla rete man mano che viene gestito. Tuttavia, con il livello di servizio completo è possibile scegliere di reindirizzare il traffico di posta in uscita attraverso i servizi Hosted Email Security.

Se si dispone di un account della registrazione in linea di Trend Micro (OLR), l'attivazione del filtro della posta in uscita è un'operazione semplice, come illustrato in *Se si dispone di un account OLR* a pagina 2-7.

Se ancora non si dispone di un account OLR, seguire le istruzioni riportate in *Se non si dispone di un account OLR* a pagina 2-8.

Domanda 18: I rivenditori e gli utenti finali possono continuare ad accedere mediante le credenziali esistenti?

Risposta: Sì. Per i rivenditori xSP e per gli utenti finali non c'è alcun cambiamento. I rivenditori xSP possono continuare a utilizzare il ruolo "per conto di" per gestire i propri utenti finali. I rivenditori xSP e gli utenti finali non possono utilizzare la schermata Gestione dominio per gestire i propri domini gestiti, tuttavia possono utilizzare la riga di comando come di consueto.

Domanda 19: Come posso modificare un nome di dominio gestito?

Risposta: Dalla schermata Gestione dominio è possibile modificare manualmente tutte le informazioni sul dominio, ad eccezione del nome di dominio. Per modificare un nome di dominio, è necessario disattivare il dominio esistente e aggiungere in nuovo nome di dominio.

Domanda 20: Come si utilizza la funzione "E-mail di prova"?

Risposta: Lo scopo della funzione "email di prova" è quello di verificare se il sistema Hosted Email Security funziona correttamente. Se per un dato intervallo di tempo non è stata ricevuto alcun messaggio e-mail, è possibile verificare se Hosted Email Security è in funzione, inviando un messaggio di prova. Se il messaggio viene ricevuto, Hosted Email Security funziona correttamente. Se il messaggio non viene ricevuto, contattare l'assistenza tecnica.

Domanda 21: Perché la schermata Gestione dominio è disattivata?

Risposta: Questo problema può verificarsi se l'accesso è stato eseguito mediante un account locale. Una volta creato un account della registrazione in linea di Trend Micro (OLR), sarà possibile accedere a Hosted Email Security utilizzando per un periodo di tempo le credenziali di accesso precedenti. Tuttavia, se si esegue l'accesso utilizzando il vecchio account, non sarà possibile apportare modifiche alla schermata Gestione dominio.

Per aggiungere un nuovo dominio o gestire un dominio gestito esistente:

1. Accedere alla pagina di accesso di Hosted Email Security.
2. Selezionare **Accedere con il nome utente e la password della registrazione in linea di Trend Micro.**
3. Inserire nome utente e password dell'account OLR.
4. Fare clic su **Accedi.** Viene visualizzata la schermata Rapporto.
5. Aggiungere o gestire il dominio come illustrato in *Gestione dei domini* a pagina 5-17.

Domanda 22: Cosa accade allo scadere della mia licenza?

Risposta: Immediatamente dopo la scadenza della licenza, inizierà un periodo consentito durante il quale il servizio continua come previsto. Al termine del periodo consentito, tuttavia, i messaggi in entrata saranno stampati con una notifica non sarà più possibile accedere alla console di amministrazione. infine, i dati saranno eliminati permanentemente. Per evitare interruzioni inutili del servizio di posta, rinnovare la licenza prima della scadenza.

Per ulteriori informazioni sulle modalità di licenza e sulla validità della licenza, vedere *Modalità di licenza* a pagina 5-35.

Appendice B

Informazioni di contatto e risorse basate sul Web

Questa appendice fornisce informazioni per ottenere ulteriore assistenza in caso di problemi tecnici.

Gli argomenti trattati nella presente appendice includono:

Contattare l’assistenza tecnica

Oltre alla guida in linea Hosted Email Security accessibile mediante la console di amministrazione, Trend Micro fornisce assistenza tecnica mediante il sito Web di Trend Micro.

Trend Micro non offre più assistenza via posta elettronica, ma mediante un sistema di invio online disponibile all’indirizzo:

http://it.trendmicro.com/it/products/enterprise/hosted-email-security/support/index.html

Sul sito indicato, è possibile reperire le informazioni più aggiornate sul servizio di assistenza nonché un collegamento alla knowledge base di Trend Micro.

I clienti che dispongono di account Hosted Email Security mediante Worry Free Business Security con Hosted Email Security possono inoltre fare riferimento ai recapiti indicati sul sito.

Informazioni di contatto generali

Ecco i numeri di telefono e di fax generali per gli Stati Uniti:

Telefono: +1 (408) 257-1500 (linea principale)

Fax: +1 (408) 257-2003

La nostra sede statunitense si trova nel cuore della Silicon Valley:

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014

Disponibilità di servizio

È possibile che di tanto in tanto si verifichino tempi di inattività programmati per motivi di manutenzione. In questi casi, viene inviata notifica scritta almeno 24 ore prima. Considerando i tempi di inattività, viene garantita una percentuale di disponibilità non inferiore al 99,99% su base annua.

Consegna e-mail

La consegna viene garantita anche se il server di posta non è temporaneamente disponibile. In caso di ripristino di emergenza a valle, il servizio continua ad analizzare ed elaborare i messaggi, i quali vengono conservati per un massimo di 5 giorni, in base al volume occupato. Quando i server di posta locali sono disponibili, i messaggi vengono consegnati con controllo intelligente del flusso per garantire la gestibilità a valle ed evitare un'inutile "inondazione" delle risorse a valle.

Knowledge Base

La Knowledge Base di Trend Micro è una risorsa in linea 24 ore su 24 e 7 giorni su 7 che contiene migliaia di procedure di assistenza tecnica fai-da-te per i prodotti e i servizi Trend Micro. La Knowledge Base si rivela utile ad esempio quando si riceve un messaggio di errore e si desidera capire cosa fare. Ogni giorno vengono aggiunte le soluzioni a nuovi problemi.

Sempre disponibili nella Knowledge Base sono le domande frequenti sui servizi, i suggerimenti importanti, i consigli preventivi antivirus e le informazioni sui contatti locali per l'assistenza e i punti vendita.

http://esupport.trendmicro.com/

Se non è possibile trovare una risposta a una particolare domanda, la Knowledge Base include un ulteriore servizio che consente di inviare la domanda tramite un messaggio e-mail. Il tempo di risposta è tipicamente di 24 ore o meno.

Invio di codice sospetto a Trend Micro

È possibile inviare a Trend Micro virus, file infetti, cavalli di Troia, worm sospetti, spyware e altri file sospetti per una valutazione. Per farlo, seguire la procedura guidata per l'invio Trend Micro all'indirizzo:

http://subwiz.trendmicro.com/SubWiz

Fare clic sul collegamento per **inoltrare un file/virus non identificato sospetto**.

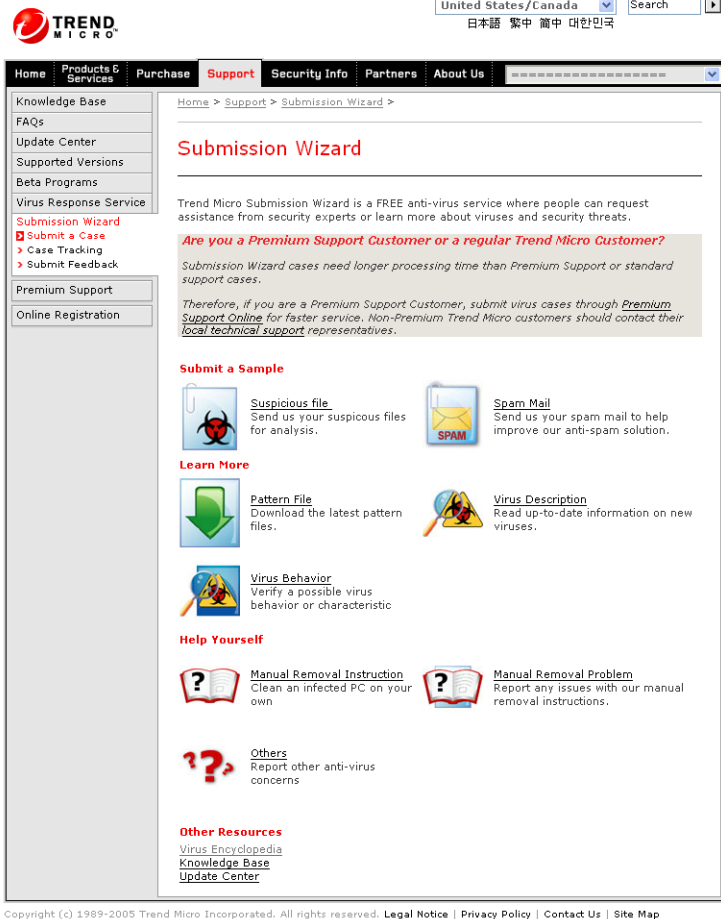



FIGURA B-22. Schermata della procedura guidata per l'invio

Viene richiesto l'inserimento delle informazioni seguenti:

- **E-mail:** l'indirizzo e-mail a cui si desidera ricevere la risposta del team dell'assistenza antivirus.
- **Prodotto:** il prodotto o servizio che si sta utilizzando. Se si utilizzano più prodotti o servizi Trend Micro, selezionare quello più rilevante per il problema oppure il prodotto o servizio più usato.
- **Numero di postazioni infette:** il numero di utenti infetti all'interno dell'organizzazione.
- **Carica file:** Trend Micro consiglia di creare un file zip protetto da password con il file infetto, utilizzando la parola "virus" come password, quindi di selezionare il file zip protetto nel campo **Carica file**.
- **Descrizione:** inserire una breve descrizione dei sintomi riscontrati. Il nostro team di tecnici specializzati nei virus esaminerà il file per identificare e definire gli eventuali rischi in esso contenuti e restituirà al più presto il file risanato, in genere entro 48 ore.

Nota: Gli invii effettuati tramite l'esperto antivirus/la procedura guidata di invio vengono indirizzati immediatamente e non sono soggetti alle politiche e alle restrizioni stabilite come parte del contratto sul livello dei servizi di reazione ai virus di Trend Micro (Virus Response Service Level Agreement, SLA).

Quando si fa clic su **Avanti**, viene visualizzata una schermata di conferma. La stessa schermata mostra anche un numero di ricerca relativo al problema inoltrato.

Se si preferisce comunicare tramite e-mail, inviare una query al seguente indirizzo:

virusresponse@trendmicro.com

Negli Stati Uniti, è possibile anche chiamare il seguente numero verde:

(877) TRENDAV o 877-873-6328

TrendLabs

TrendLabs è l'infrastruttura globale dei centri Trend Micro per la ricerca antivirus e l'assistenza tecnica che fornisce ai clienti informazioni tempestive sulla sicurezza.

Gli esperti antivirus TrendLabs monitorano potenziali rischi per la sicurezza nel mondo, per assicurare che i prodotti e i servizi Trend Micro siano sicuri contro i rischi emergenti. Il culmine giornaliero di questi sforzi condiviso con i clienti attraverso frequenti aggiornamenti dei file di pattern antivirus e miglioramenti al motore di scansione.

Il personale di TrendLabs è costituito da un team composto da diverse centinaia di ingegneri e personale qualificato per l'assistenza in grado di offrire un'ampia gamma di prodotti e servizi. I Centri servizi dedicati e i team di rapida risposta hanno sede a Tokyo, Manila, Taipei, Monaco, Parigi e Lake Forest (California).

Centro informazioni sulla sicurezza

Per informazioni esaurienti sulla sicurezza è possibile visitare gratuitamente il sito Web informativo sulla sicurezza Trend Micro all'indirizzo:

http://www.trendmicro.com/vinfo/it/virusencyclo/default.asp

Visitare il sito informativo sulla sicurezza per:

- Leggere la relazione settimanale sui virus, che include un elenco di rischi la cui attivazione è prevista nella settimana corrente e descrive i 10 rischi prevalenti al mondo per la settimana attuale.
- Consultare l'Enciclopedia dei virus, un elenco dei rischi noti che include la classe di rischio, i sintomi delle infezioni, le piattaforme esposte, la routine dei danni e le istruzioni su come rimuovere il rischio, nonché informazioni sui messaggi "bufala" relativi ai computer.
- Scaricare i file di prova dall'European Institute of Computer Anti-virus Research (EICAR), per verificare se il prodotto o servizio di sicurezza è correttamente configurato.
- Leggere le informazioni di carattere generale, comprendenti:
  - Il Virus Primer, che aiuta a comprendere la differenza tra virus, cavalli di Troia, worm e altri rischi.
  - La Guida per *l'uso sicuro del computer di Trend Micro.*

- Una descrizione delle classi di rischio, per comprendere il danno potenziale di un rischio classificato come Molto basso o Basso rispetto a uno classificato come Medio o Alto.
- Un glossario di virus e altra terminologia relativa ai rischi per la sicurezza.
- Scaricare i documenti tecnici sul settore globale.

MALWARE NAME	RISK RATING	ADVISORY DATE	PATTERN FILE
WORM_ONLINEG.DJO	Low	Jan 30, 2008	4.969.00
WORM_IRCBOT.SN	Low	Jan 26, 2008	4.957.00
WORM_AGENT.TBH	Low	Jan 25, 2008	4.579.00
SYMBOS_BESELO.A	Low	Jan 23, 2008	4.961.00
WORM_IMBOT.AC	Low	Jan 22, 2008	4.961.00
BKDR_IRCBOT.RB	Low	Jan 22, 2008	4.957.00
HTML_IFRAME.IY	Low	Jan 18, 2008	4.949.00
WORM_NUWAR.BK	Low	Jan 15, 2008	4.967.00
TROJ_AGENT.HJS	Low	Jan 13, 2008	4.957.00
TROJ_DROPPER.NH	Low	Jan 13, 2008	4.943.00

FIGURA B-23. Schermata delle informazioni sulla sicurezza di Trend Micro

- È possibile iscriversi gratuitamente al servizio di rilevamento dei virus di Trend Micro, per venire a conoscenza delle infezioni non appena si verificano, e al rapporto settimanale sui virus
- Sono disponibili informazioni sugli strumenti gratuiti di aggiornamento dei virus disponibili per i webmaster

Appendice C

Introduzione a Web EUQ

Questa appendice fornisce informazioni utili per la comprensione e l'uso del servizio Hosted Email Security Web End-User Quarantine. Contiene la versione integrale della *Guida per l'utente di Trend Micro Web End User Quarantine*, scaricabile separatamente come manuale in formato PDF.

Hosted Email Security Web End-user Quarantine (EUQ) è un'interfaccia utente che facilita la gestione dei messaggi e-mail contenenti spam messi in quarantena. Inoltre, consente di impostare un elenco di mittenti approvati i cui messaggi devono essere consegnati e non messi in quarantena. L'uso è estremamente semplice, come mostrato nella *figura C-1*.

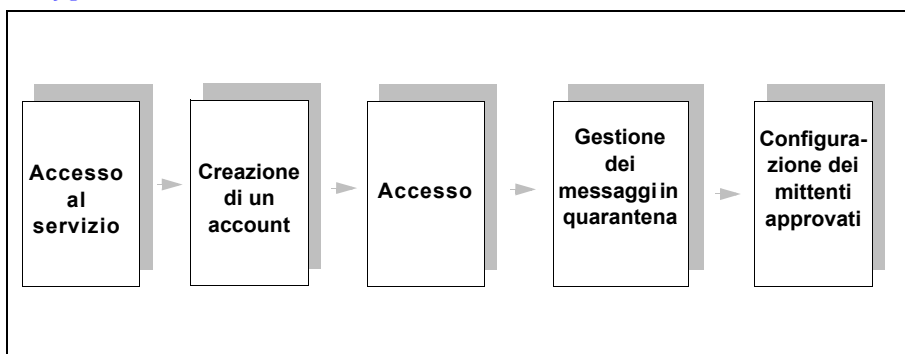



FIGURA C-1. Introduzione a Hosted Email Security Web EUQ

Accesso a Web End User Quarantine

L'accesso a Web End User Quarantine richiede una connessione a Internet e uno dei browser seguenti:

- Microsoft™ Internet Explorer™, versione minima 6.0
- Mozilla™ Firefox™, versione minima 2.0

Per accedere al servizio procedere come segue.

1. Aprire il browser.
2. Accedere all'URL fornito dall'amministratore di sistema.

Creazione di un account

Per utilizzare Web EUQ, è necessario disporre di un account.

Per registrare un nuovo account procedere come segue.

1. Accedere al servizio.
2. Fare clic sul collegamento **Registra nuovo account** nella pagina di accesso visualizzata in *figura C-2*.

FIGURA C-2. Schermata di accesso di Hosted Email Security Web EUQ

3. Inserire nome e cognome nei campi delle informazioni personali visualizzati nella *figura C-3*.

FIGURA C-3. Schermata Creazione di un nuovo account

4. Inserire e confermare l'indirizzo e-mail nei campi delle informazioni di accesso.
5. Inserire due volte la password da associare al nuovo account.
6. Selezionare una domanda di sicurezza e immettere la risposta.
7. Inserire il testo indicato nell'immagine.
8. Fare clic su **Fine**.

Dopo l'autenticazione delle informazioni, l'utente riceverà un messaggio e-mail contenente un URL di attivazione. Fare clic sull'URL per attivare la nuova password. Accedere alla console Web EUQ con la password stabilita nel *Passaggio 5*.

Accesso a Hosted Email Security Web End User Quarantine

Una volta creato un nuovo account, verrà inviato un messaggio e-mail che conferma l'autenticazione delle informazioni e la creazione dell'account.

Per accedere la prima volta a Web End User Quarantine procedere come segue.

1. Aprire il messaggio e-mail ricevuto in cui si conferma la creazione dell'account.
2. Fare clic sull'URL di attivazione.

   Viene visualizzata la schermata di accesso a Web EUQ mostrata nella *figura C-2*.
3. Immettere l'indirizzo e-mail utilizzato per impostare l'account.
4. Immettere la password selezionata quando è stato creato l'account.
5. Fare clic su **Accedi**.

Operazioni eseguibili sullo spam in quarantena

La schermata Spam in quarantena è la prima schermata ad essere visualizzata quando si accede a Web EUQ. In questa schermata è possibile eseguire le operazioni indicate.

- Visualizzare e ordinare un elenco di messaggi in quarantena che sono stati bloccati prima di raggiungere la posta in arrivo
- Eseguire sui messaggi in quarantena una delle tre azioni opzionali indicate:
  - Elimina
  - Recapita (non spam)
  - Recapita e approva mittente

La schermata Spam in quarantena mostra, sopra la tabella, il numero di indirizzi di mittenti attualmente approvati. Per informazioni su come aggiungere o modificare gli indirizzi dei mittenti approvati, fare riferimento a *Uso della schermata Mittenti approvati* a pagina C-6.

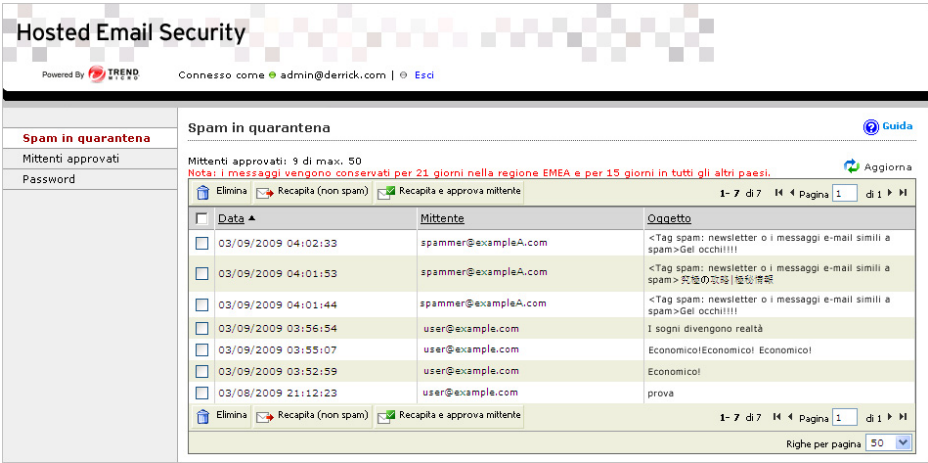



FIGURA C-4. Schermata Spam in quarantena

Per visualizzare e ordinare gli elementi in quarantena nella tabella procedere come segue.

1. Opzionalmente, nascondere/visualizzare il numero di messaggi mostrati (10, 25, 50, 100, 250, 500) utilizzando l'elenco a discesa a destra sotto la tabella.
2. Navigare tra i messaggi facendo clic sulle immagini a destra della riga dell'intestazione secondo le indicazioni di seguito.
   - |< prima pagina
   - < indietro di una pagina
   - > avanti di una pagina
   - |> ultima pagina
3. Disporre i messaggi in ordine crescente o decrescente per le seguenti categorie:
   - Data e ora di ricezione (gg/mm/aa, hh:mm:ss)
   - Indirizzo del mittente
   - Oggetto

Per eseguire una delle tre azioni per gli elementi in quarantena:

1. Selezionare i messaggi in questione in uno dei modi seguenti:
   - Selezionare le caselle di controllo a sinistra di ogni voce.
   - Selezionare la casella di controllo a sinistra dell'intestazione della colonna "Data" per selezionare tutti i messaggi nella pagina visualizzata.
2. Selezionare un'azione da eseguire.
   - **Elimina ( ):** i messaggi selezionati vengono eliminati.
   - **Recapita (non spam) ( ):** i messaggi selezionati vengono inviati all'account e-mail personale.
   - **Recapita e approva mittente ( ):** i messaggi selezionati vengono inviati all'account e-mail personale e l'indirizzo del mittente viene aggiunto all'elenco di mittenti approvati.

Nota: Trend Micro Hosted Email Security conserva i messaggi in quarantena fino a 21 giorni nella regione EMEA e 15 giorni in tutti gli altri paesi. Al termine del periodo indicato, i messaggi verranno eliminati.

Uso della schermata Mittenti approvati

Nella schermata Mittenti approvati è possibile eseguire le operazioni indicate.

- Visualizzare un elenco dei mittenti approvati esistenti ed eseguire un ordinamento per data di approvazione o indirizzo del mittente
- Approvare indirizzi specifici o domini per inviare messaggi al proprio indirizzo e-mail
- Eliminare indirizzi o domini esistenti relativi ai mittenti approvati
- Modificare indirizzi o domini esistenti relativi ai mittenti approvati

Quando si utilizza la schermata Mittenti approvati, si applicano le condizioni elencate di seguito.

- Hosted Email Security può contenere un massimo di 50 mittenti approvati nell'elenco.
- Email Reputation Services (ERS) non blocca eventuali messaggi e-mail provenienti dai mittenti (o domini) specificati.
- Le regole anti-spam euristiche basate sul contenuto non vengono applicate ai messaggi e-mail ricevuti dai mittenti o dai domini specificati.
- Tutte le regole relative a virus, contenuto e allegati impostate dall'amministratore vengono comunque applicate.

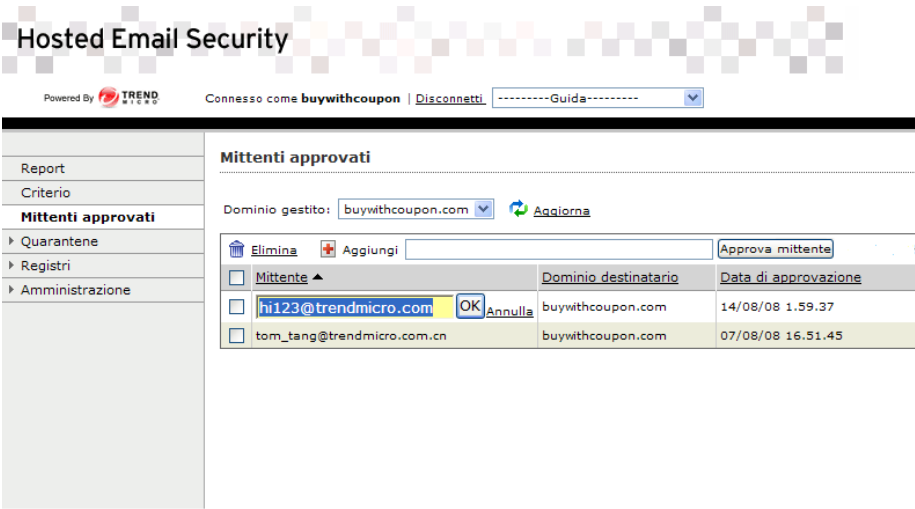



FIGURA C-5. Modifica di un indirizzo nella schermata Mittenti approvati

Ordinamento delle voci di messaggio

È possibile visualizzare i mittenti approvati esistenti in ordine crescente o decrescente sulla base dei criteri indicati.

- Data e ora di approvazione (gg/mm/aa, hh:mm:ss)
- Indirizzo del mittente

Aggiunta o modifica dei mittenti approvati

Per aggiungere un mittente approvato:

1. Immettere un singolo indirizzo o dominio nel campo **Aggiungi**.
    - Per un singolo indirizzo, utilizzare il seguente modello: nome@esempio.com
    - Per un dominio, utilizzare il seguente modello: *@esempio.com

Nota: Il carattere jolly asterisco è accettato solo nella posizione che precede il simbolo "@". I due esempi illustrati sopra sono gli unici formati consentiti come mittenti approvati. Non sono accettate voci del tipo *@* o altri formati di indirizzo variabili.

2. Fare clic su **Aggiungi**.

Per modificare gli indirizzi e/o i domini esistenti relativi ai mittenti approvati:

1. Fare clic sul collegamento dell'indirizzo e-mail da modificare.

   Il collegamento si trasforma in un campo modificabile.
2. Modificare l'indirizzo o il dominio.
3. Fare clic su **Invia** per salvare l'indirizzo o il dominio modificato.

Modifica della password

Trend Micro consiglia di cambiare periodicamente la password. Inoltre, Web End User Quarantine (EUQ) richiede una password di lunghezza compresa tra 8 e 32 caratteri.

Web EUQ consente di modificare la password in due modi.

- *Per modificare la password se la si conosce:*
- *Per reimpostare la password:*

Per modificare la password se la si conosce:

1. Fare clic su **Password** nel menu a sinistra.
2. Digitare la password vecchia/corrente.

Nota: Trend Micro consiglia vivamente di utilizzare password contenenti più tipi di carattere (una combinazione di lettere, numeri e caratteri speciali).

3. Immettere e confermare la nuova password.
4. Fare clic su **Salva**.

Per reimpostare la password di Web EUQ, è necessario ricordare la domanda di sicurezza inserita durante la creazione dell'account. Se non si ricordano la domanda e la risposta, si può chiedere all'amministratore di sistema di intervenire e di reimpostare la password.

Per reimpostare la password:

1. Nella **schermata di accesso** fare clic sul collegamento **Password dimenticata?**. Viene visualizzata la schermata mostrata nella *figura C-6*.

FIGURA C-6. Finestra di dialogo Password dimenticata

2. Se si dispone di un account della registrazione in linea di Trend Micro (OLR), selezionare **Sì**, e Web EUQ reindirizza l'utente alla pagina "Password dimenticata" del sito OLR.
3. Se non si dispone di un account OLR, fare clic su **No**. Viene visualizzata la schermata mostrata nella figura C-7 a pagina C9.

FIGURA C-7. Schermata Reimpostazione della password per gli utenti che non hanno un account OLR

4. Inserire nome utente e indirizzo e-mail di Hosted Email Security.

Nota: L'indirizzo e-mail deve corrispondere all'indirizzo e-mail del contatto immesso all'attivazione del servizio.

5. Immettere il testo indicato nell'immagine di verifica CAPTCHA.
6. Fare clic su **Salva**. Dopo l'autenticazione delle informazioni, l'utente riceverà un messaggio e-mail contenente un URL di attivazione.
7. Fare clic sull'URL di attivazione nel messaggio e-mail. Web EUQ attiva la nuova password e visualizza una pagina di conferma.
8. Fare clic su **Continua** nella pagina di conferma e accedere alla console utilizzando la password stabilita nel *Passaggio 5*.

Nota: Se non è possibile autenticare le informazioni, la password non verrà reimpostata. Se si dimentica l'indirizzo e-mail originale o la domanda di sicurezza, contattare l'amministratore di sistema. L'amministratore di sistema può effettuare la reimpostazione della password.

Glossario

Questo glossario illustra i termini particolari utilizzati nel presente documento o nella guida in linea.

Termine	**Spiegazione**
account amministratore	Un nome utente e una password con privilegi di amministratore.
adware	Software sovvenzionato dalla pubblicità in cui gli annunci pubblicitari vengono visualizzati quando il programma è in esecuzione. L'Adware installa un "backdoor". Il software che controlla le attività svolte nel computer dell'utente in assenza del consenso dell'utente stesso è detto "spyware".
amministratore	Si riferisce all'"amministratore di sistema": la persona, all'interno dell'organizzazione, responsabile per attività quali l'impostazione di un nuovo hardware e software, l'allocazione di utenti e password, il monitoraggio dello spazio su disco e di altre risorse IT, l'esecuzione dei backup e la gestione della protezione della rete.
antivirus	Programmi progettati per rilevare e disinfettare il computer dai virus.
archivio	Un unico file contenente uno o (generalmente) più file distinti oltre alle informazioni che ne consentono l'estrazione (separata) per mezzo di un programma idoneo, ad esempio un file .zip.
attacco DoS (Denial of Service)	Messaggi e-mail con allegati di grandi dimensioni indirizzati a un gruppo, i quali intasano le risorse della rete fino a causare il forte rallentamento, se non l'interruzione, del servizio di messaggistica.
attiva	Per attivare il software una volta completato il processo di registrazione. I prodotti Trend Micro non saranno operativi fino al completamento dell'attivazione. Attivare durante o dopo l'installazione (nella console di gestione) dalla schermata Licenza del prodotto.

TERMINE	SPIEGAZIONE
autenticazione	La verifica dell'identità di una persona o di un processo. L'autenticazione garantisce che la trasmissione dei dati digitali sia indirizzata al destinatario desiderato. Inoltre, l'autenticazione garantisce al destinatario l'integrità del messaggio e consente di visualizzarne la fonte (da dove proviene o chi sia il mittente). La forma più semplice di autenticazione richiede un nome utente e una password, al fine di accedere a un particolare account. I protocolli di autenticazione si possono basare sulla crittografia a chiave privata, ad esempio l'algoritmo Data Encryption Standard (DES) o su un sistema di chiavi pubbliche mediante le firme digitali. *Vedere anche* crittografia a chiave pubblica *e* firma digitale.
avvia	Un evento che causa il verificarsi di un'azione. Ad esempio, il prodotto Trend Micro in uso rileva un virus all'interno di un messaggio e-mail. Tale rilevamento può portare il prodotto o servizio ad *avviare* la messa in quarantena del messaggio e a inviare una notifica all'amministratore del sistema, al mittente e al destinatario del messaggio.
azione (*Vedere anche* notifica)	L'operazione può essere eseguita se: • è stato rilevato un virus • sono stati rilevati messaggi di spam • si è verificata una violazione dei contenuti • è stato effettuato un tentativo di accesso a un URL bloccato oppure • è stato attivato un blocco del file. Fra le azioni, in genere, sono inclusi la disinfezione e il recapito, la quarantena, l'eliminazione o l'invio/trasferimento in ogni caso. L'invio/trasferimento in ogni caso è sconsigliato: l'invio di un messaggio contenente virus o il trasferimento di un file infettato da virus può compromettere la rete.

TERMINE	SPIEGAZIONE
blocca	Per impedire che altri accedano alla rete.
carico utile	Il carico utile fa riferimento a un’azione eseguita da un virus sul computer infetto. Tale azione può risultare relativamente innocua, nel caso della visualizzazione di messaggi o di eventuali espulsioni dell’unità CD, o al contrario del tutto dannosa, come avviene, ad esempio, per l’eliminazione dell’intero disco rigido.
client	Un sistema o un processo che richiede il supporto di un altro sistema o processo (un "server") mediante un protocollo e ne accetta le risposte. Un client fa parte di un’architettura software client-server.
Codice di attivazione	Un codice di 37 caratteri, trattini inclusi, utilizzato per attivare i prodotti Trend Micro. Di seguito viene riportato un esempio di codice di attivazione: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Vedere anche* Chiave di registrazione.
configurazione	La selezione delle opzioni in base alle quale il prodotto Trend Micro funzionerà, ad esempio, se si sceglie di mettere in quarantena o di eliminare un messaggio e-mail infetto da virus.
console di gestione	L’interfaccia utente per il prodotto o servizio Trend Micro in uso.
criteri	I criteri forniscono il meccanismo iniziale di protezione del firewall e consentono di determinare il traffico che lo attraversa sulla base dei dettagli della sessione IP. Permettono inoltre di proteggere la rete attendibile dagli attacchi esterni, ad esempio la scansione dei server trusted. I criteri creano un ambiente nel quale impostare i criteri di protezione, al fine di monitorare il traffico che tenta di attraversare il firewall in uso.

TERMINE	SPIEGAZIONE
crittografia	La crittografia è il processo di modifica dei dati in modo tale che questi siano leggibili unicamente dal destinatario desiderato. Al fine di decifrare il messaggio, il destinatario dei dati crittografati deve disporre della chiave di decrittografia appropriata. Negli schemi crittografici tradizionali, il mittente e il destinatario utilizzano la stessa chiave per crittografare e decrittografare i dati. Gli schemi di crittografia a chiave pubblica utilizzano due chiavi: una chiave pubblica, utilizzabile da tutti, e una chiave privata corrispondente, la quale è utilizzabile unicamente dalla persona che la ha creata. In questo modo chiunque può inviare un messaggio crittografato mediante la chiave pubblica del proprietario, tuttavia solo il proprietario disporrà della chiave privata necessaria a decrittografarlo. PGP (Pretty Good Privacy) e DES (Data Encryption Standard) sono i due schemi di crittografia a chiave pubblica maggiormente utilizzati.
crittografia a chiave pubblica	Uno schema crittografico in cui ciascuna persona dispone di una coppia di "chiavi", denominate rispettivamente chiave pubblica e chiave privata. La chiave pubblica di ciascuna persona viene pubblicata, al contrario la chiave privata rimane segreta. I messaggi vengono crittografati mediante la chiave pubblica del destinatario desiderato e può essere decrittografata unicamente mediante la sua chiave privata. *Vedere anche* autenticazione *e* firma digitale.
disinfetta	Per rimuovere il codice dannoso da un file o da un messaggio.
DNS	Domain Name System: un servizio di query di dati, utilizzato principalmente in Internet per la traduzione dei nomi host in indirizzi IP.
dominio (amministrativo)	Un gruppo di computer che condivide un database e criteri di protezione comuni.

TERMINE	SPIEGAZIONE
DUL (Dynamic User List)	Associato a Trend Micro Email Reputation Services, questo elenco contiene indirizzi IP assegnati dinamicamente oppure gli indirizzi con un criterio di utilizzo accettabile che proibisce i server di posta pubblici.
End User License Agreement (EULA)	Il Contratto di licenza con l'utente finale (End User License Agreement o EULA) è un contratto legale fra l'autore o distributore di software e l'utente del software stesso. Normalmente tale contratto definisce le restrizioni cui l'utente è sottoposto; l'utente potrà rifiutare le condizioni dell'accordo semplicemente non selezionando il pulsante "Accetto", al momento dell'installazione. Se si seleziona "Non accetto", ovviamente, l'installazione del prodotto software non verrà completata. Quando selezionano "Accetto" all'interno delle finestre di conferma del contratto di licenza con l'utente finale EULA visualizzate durante l'installazione di alcuni software gratuiti, molti utenti acconsentono inavvertitamente all'installazione di spyware e adware nel computer.
End User Quarantine (EUQ, Web EUQ)	Anche denominata Web EUQ, un interfaccia utente basata sul Web che permette agli utenti finali di gestire i messaggi e-mail di spam messi in quarantena.
Ethernet	La tecnologia LAN (local area network) ideata da Xerox Corporation, Palo Alto Research Center. Ethernet è un sistema di recapito di tipo best-effort che sfrutta la tecnologia CSMA/CD. È possibile eseguire Ethernet su una varietà di schemi di collegamenti cavo, inclusi il cavo coassiale spesso e il cavo coassiale sottile, il cavo a coppini intrecciati e il cavo a fibre ottiche. Ethernet rappresenta uno standard per la connessione dei computer all'interno di una rete locale. La rete Ethernet più diffusa è denominata 10BaseT, che indica una velocità di trasmissione di picco pari a 10 Mbps mediante un cavo a coppini intrecciati di rame.
EUQ	Vedere *End User Quarantine*.

TERMINE	SPIEGAZIONE
falso positivo	Un messaggio e-mail "intercettato" dal filtro anti-spam e identificato come spam, anche se in effetti non lo è.
file compresso	Un unico file contenente uno o più file distinti, oltre alle informazioni che ne consentono l'estrazione per mezzo di un programma idoneo, ad esempio WinZip.
file di pattern (anche noto come Official Pattern Release)	Il file di pattern, anche denominato Official Pattern Release (OPR), è l'ultima compilazione dei pattern di scansione per le minacce identificate. Ha superato una serie di test critici per garantire la protezione ottimale dalle minacce di ultima generazione. Questo file di pattern è più efficace se utilizzato in combinazione il motore di scansione più recente.
filtro del contenuto	Scansione dei messaggi e-mail alla ricerca di contenuti (parole o frasi) proibiti dal dipartimento delle risorse umane dell'organizzazione o dai criteri di messaggistica IT, ad esempio messaggi con contenuti violenti, blasfemi o pornografici.
filtro posta in uscita	Una funzione facoltativa di Hosted Email Security che filtra i messaggi e-mail contenenti spam. Questa funzione deve essere attivata prima della crittografia e-mail.
firewall	Un dispositivo gateway con misure di sicurezza particolari, utilizzato per veicolare le connessioni esterne (particolarmente Internet) e le linee dial-in.
firma digitale	I dati aggiuntivi di un messaggio, i quali consentono di identificare e autenticare il mittente e i dati del messaggio mediante una tecnica denominata crittografia a chiave pubblica. *Vedere anche* crittografia a chiave pubblica *e* autenticazione.
gateway	Un'interfaccia un'origine informazioni e un server Web.
guida in linea	La documentazione è accompagnata da un'interfaccia utente grafica.

TERMINE	**SPIEGAZIONE**
host	Un computer connesso alla rete.
HTTP	Hypertext Transfer Protocol: il protocollo TCP/IP server-client utilizzato sul Web per lo scambio di documenti HTML. Per convenzione, a questo scopo viene utilizzata la porta 80.
HTTPS	Hypertext Transfer Protocol Secure: una variante del protocollo HTTP, utile per la gestione delle transazioni protette.
Chiave di registrazione	Un codice di 22 caratteri, inclusi trattini, utilizzato in alcune aree per eseguire la registrazione nel database dei clienti Trend Micro. Di seguito viene riportato un esempio di chiave di registrazione: SM-27RT-UY4Z-39HB-MNW8 *Vedere anche* Codice di attivazione.
in entrata	Messaggi e-mail o altri dati indirizzati *alla* rete in uso.
in uscita	Messaggi e-mail o altri dati che *lasciano* la rete e sono reindirizzati su Internet.
indirizzo e-mail dell'amministratore	Questo indirizzo viene utilizzato dall'amministratore del prodotto Trend Micro per gestire le notifiche e gli avvisi.
Internet Protocol (IP)	Un protocollo Internet standard che definisce un'unità di dati di base denominata datagramma. Un datagramma viene utilizzato all'interno di un sistema di recapito best-effort senza connessione. Il protocollo Internet definisce le modalità con cui le informazioni vengono distribuite ai vari sistemi attraverso Internet.
intestazione (definizione di networking)	Parte di un pacchetto di dati contenente informazioni chiare sul file o sulla trasmissione.

TERMINE	SPIEGAZIONE
KB	Kilobyte: 1.024 byte di memoria.
LDAP (Lightweight Directory Access Protocol)	Un protocollo Internet utilizzato dai programmi di posta elettronica per individuare le informazioni di contatto provenienti da un server. Ad esempio, supponiamo che si desideri individuare tutte le persone che a Boston dispongono di un indirizzo e-mail contenente il nome "Bob". Una ricerca LDAP consentirebbe di visualizzare gli indirizzi e-mail che soddisfano tali criteri.
licenza	Autorizzazione legale all'utilizzo dei prodotti o servizi Trend Micro.
malware (software dannoso)	Programmi o file sviluppati allo scopo di danneggiare il sistema, fra questi vi sono i virus, i worm e i cavalli di Troia.
MB	Megabyte: 1.024 kilobyte di dati.
motore di scansione	Il modulo che esegue la scansione delle minacce e il rilevamento nel prodotto nel quale è integrato.
MTA (Mail Transfer Agent)	Il programma responsabile della consegna dei messaggi e-mail. *Vedere anche* Server SMTP.
nome dominio	Il nome completo di un sistema, composto dal nome host locale e dal nome di dominio, ad esempio, tellsitall.com. Un nome di dominio è sufficiente per determinare un indirizzo Internet univoco per tutti gli host di Internet. Tale processo, denominato "risoluzione nomi", utilizza il Domain Name System (DNS).
notifica (*Vedere anche* azione e destinazione)	Un messaggio inoltrato a una o più delle seguenti figure: • amministratore di sistema • mittente di un messaggio • destinatario di un messaggio, del download o del trasferimento di un file

TERMINE	SPIEGAZIONE
OPS (Open Proxy Stopper)	Associato a Trend Micro Email Reputation Services, questo elenco contiene gli indirizzi IP dei server aperti come server proxy e origine di spam note.
postazione	Una licenza di una persona per l'utilizzo del prodotto Trend Micro.
proxy	Un processo che fornisce una cache di elementi disponibili su altri server presumibilmente più lenti o costosi.
QIL (Quick IP List)	Il nome originario del database di reputazione dinamica di Trend Micro Email Reputation Services.
RBL (Real-time Blackhole List)	È un elenco di indirizzi IP di server di posta, noti come origine di spam.
registrazione	Il processo di identificazione in qualità di cliente Trend Micro; in alcune aree si effettua utilizzando la chiave di registrazione di un prodotto, nella schermata della registrazione in linea di Trend Micro. https://olr.trendmicro.com/registration
risoluzione DNS	Se un client DNS richiede i nomi host e i dati indirizzo da un server DNS, il processo viene denominato risoluzione. In un server che esegue la risoluzione predefinita ha luogo la configurazione DNS di base. Ad esempio, un server remoto richiede a un altro server i dati su un computer nella zona corrente. Il software client del server remoto interroga il sistema di risoluzione, il quale risponde alla richiesta mediante i propri file di database.
routine dei danni	La porzione dannosa del codice virale, anche denominata carico utile.
RSS	Vedere *Relay Spam Stopper.*

TERMINE	SPIEGAZIONE
RSS (Relay Spam Stopper)	Associato a Trend Micro Email Reputation Services, questo elenco contiene gli indirizzi IP dei server di posta aperti come relay di posta e origine di spam note.
scansione basata su regole euristiche	Scansione del traffico di rete che utilizza un'analisi logica delle proprietà, la quale riduce o limita la ricerca.
server proxy	Un server Web che accetta gli URL con un prefisso particolare, utile per recuperare documenti da una cache locale o da un server remoto. Una volta eseguita questa operazione, restituisce l'URL al richiedente.
Server SMTP	Un server che inoltra i messaggi e-mail ad altre destinazioni.
SMTP	Simple Mail Transfer Protocol: un protocollo utilizzato per trasferire la posta elettronica fra computer, generalmente mediante Ethernet. Si tratta di un protocollo server-server, in questo modo gli altri protocolli vengono utilizzati per accedere ai messaggi.
SNMP	Simple Network Management Protocol: un protocollo che supporta il monitoraggio dei dispositivi collegati a una rete in condizioni che meritano l'attenzione dell'amministratore.
spyware	Software sovvenzionato dalla pubblicità che in genere installa un software di monitoraggio nel sistema, capace di inviare le informazioni sull'utente a terzi. Il pericolo consiste nel fatto che gli utenti non possono sapere quali siano i dati raccolti o come vengano utilizzati.
tipo di file	Il tipo di dati archiviati in un file. La maggior parte dei sistemi operativi utilizza l'estensione del nome di file per determinare il tipo di file. Il tipo di file viene utilizzato per scegliere un'icona appropriata al fine di rappresentare il file stesso in un'interfaccia utente, oltre all'applicazione corretta mediante la quale visualizzare, modificare, eseguire o stampare il file.

TERMINE	SPIEGAZIONE
Trap SNMP	Il trap è un meccanismo di programmazione che gestisce gli errori o altri problemi all'interno di un programma. Un trap SNMP gestisce gli errori connessi al monitoraggio delle periferiche di rete. *Vedere* SNMP.
violazione dei contenuti	Un evento che ha attivato i criteri di filtro dei contenuti.
virus	Un virus è un programma (una porzione di codice eseguibile) che dispone della capacità unica di infettare. Esattamente come i virus biologici, i virus informatici possono diffondersi rapidamente e, spesso, sono complessi da estirpare. Oltre alla capacità di replicarsi, alcuni virus hanno in comune un altro fattore: una routine dei danni che diffonde il carico utile del virus. Se il carico utile è in grado solo di far visualizzare messaggi o immagini, i virus possono distruggere i file, riformattare il disco rigido o causare altri danni. Anche se il computer non contiene una routine dei danni, questa può generare problemi, consumando lo spazio di archiviazione e la memoria del computer e limitarne le prestazioni in genere.
Web EUQ	Vedere *End User Quarantine*.
zona	Una zona è un segmento dello spazio di rete al quale sono applicate le misure di sicurezza (una zona di sicurezza), un segmento logico al quale è collegata un'interfaccia del tunnel VPN (una zona di tunnel) oppure un'entità fisica o logica con funzioni specifiche (una zona di funzione).

Indice

Simboli

A

B

C

D

E

O

P

Q

R

S

T